

EINDRAPPORTAGE

Uitvoeringstoets Wdo

Een onderzoek naar de impact van de invoering van de Wet digitale overheid (Wdo) op provincies en waterschappen

18 augustus 2021

EINDRAPPORTAGE

Uitvoeringstoets Wdo

Een onderzoek naar de impact van de invoering van de Wet digitale overheid (Wdo) op provincies en waterschappen

Harro Spanninga
Rosa-May Postma
Dirk Jan Schoneveld

18 augustus 2021

Inhoudsopgave

Samenvattende conclusies en aanbevelingen 4

1. Inleiding 12

1.1	Context en achtergrond.....	12
1.2	Reikwijdte van uw vraag aan Berenschot.....	12
1.3	Onderzoeksvragen	13
1.4	Leeswijzer.....	13

2. Onderzoeksopzet.....14

2.1	Methode en opzet van het onderzoek.....	14
2.2	Survey en workshops.....	14
2.3	Geconsulteerde functionarissen.....	15

Veranderingen Wdo en juridische analyse16

3.1	Wet digitale overheid	16
3.2	Wettelijke verplichtingen	18
3.3	Samenhang met andere wetgeving.....	22

4. Impact op provincies en waterschappen..... 23

4.1	Impact dienstverlening.....	23
4.2	Tussenconclusies dienstverlening.....	27
4.3	Impact informatieveiligheid en ICT.....	27
4.4	Tussenconclusies Informatiebeveiliging en ICT.....	30
4.5	Impact bestuur en organisatie.....	30
4.6	Impact financieel.....	31
4.7	Tussenconclusies bestuur, organisatie en financieel.....	32

Bijlage 1 Begeleidingsgroep en gesprekspartners..... 33

Samenvattende conclusies en aanbevelingen

Dit document vormt de eindrapportage van de uitvoeringstoets die Berenschot heeft gedaan op de Wet digitale overheid (Wdo), in opdracht van het IPO en de UvW. Het geeft duiding aan de impact van invoering van de wet op provincies, waterschappen en hun samenwerkingsverbanden. We beginnen dit document met een samenvatting van de conclusies en aanbevelingen van het onderzoek, door antwoord te geven op zeven centrale onderzoeksvragen. Na de samenvatting volgt een nadere uitwerking van de wijze waarop we tot deze conclusies en aanbevelingen zijn gekomen.

Vraag 1: Wat betekent de Wet Digitale Overheid voor provincies en waterschappen?

De Nederlandse samenleving digitaliseert. Dit betekent dat steeds meer transacties digitaal plaatsvinden, ook met de overheid. Het is belangrijk om te zorgen dat dit veilig en overzichtelijk kan. Het wetsvoorstel Wet digitale overheid (Wdo) legt de basis voor deze digitalisering van de overheid (voorheen de Wet Generieke Digitale Infrastructuur (Wgdi)). De Wdo heeft als doel het regelen van veilig en betrouwbaar inloggen voor Nederlandse burgers en bedrijven bij de (semi) overheid¹.

De Wdo is een zogeheten kaderwet, dit betekent dat de wet algemene principes, verantwoordelijkheden en procedures regelt, maar geen gedetailleerde uitwerking. De uitwerking vindt plaats in lagere regelgeving. In deze uitvoeringstoets zijn de gevolgen van deze nadere regelgeving onderzocht. Samenvattend geformuleerd vereisen de actueel voorliggende regels dat provincies en waterschappen:

- Zorgdragen dat alle publiek toegankelijke websites van provincies en waterschappen voldoen aan een minimale set van eisen voor beveiligde verbindingen;
- Alle erkende en toegelaten inlogmiddelen accepteren waarmee ondernemers en inwoners van Europa diensten elektronisch willen afnemen van provincies of waterschappen;

- Zorgdragen dat voor alle elektronische diensten het passende niveau voor toegangsbeveiliging wordt gebruikt afhankelijk van de soort gegevens die worden verwerkt;
- Diensten digitaal kunnen leveren via een wettelijke of vrijwillig gemachtigde vertegenwoordiger;
- Borgen dat de informatieveiligheid voor deze elektronische diensten afdoende is geregeld door het invoeren van een aantal beveiligingsmaatregelen.

Op basis van verkennende gesprekken, een survey en een aantal workshops, zijn de onderzoeksvragen beantwoordt. Aan de hand van de onderzoeksvragen presenteren wij onze conclusies en aanbevelingen van de uitvoeringstoets. We geven ons gewogen antwoord op de onderzoeksvragen op basis van de verzamelde informatie.

Vraag 2: Wat wijzigt er door de nieuwe regelgeving in de verplichtingen en werkwijze van de waterschappen, provincies en hun samenwerkingsverbanden?

Op hoofdlijnen verandert de Wdo in beginsel niets aan de werkwijzen en de verantwoordelijkheidsverdeling van de waterschappen, provincies en hun samenwerkingsverbanden op het gebied van digitale dienstverlening. De Wdo sluit aan bij de ontwikkelingen van de afgelopen jaren en wat hierover interbestuurlijk is afgesproken. Deze afspraken zijn bijvoorbeeld vastgelegd in de 'pas toe of leg uit lijst' van het Forum Standaardisatie. Op onderdelen introduceert de Wdo wel enkele nieuwe elementen.

De wet maakt het gebruik van een versleuteld BSN mogelijk. Dat is nu nog niet het geval. Dit betekent dat wanneer het gebruik van een versleuteld BSN geïntroduceerd wordt, het BSN ontcijferd moet worden. Vooralsnog gebeurt dit binnen het identificatiestelsel. Door versleuteling is de privacy bij het verstrekken van het BSN via een privaat inlogmiddel beter geborgd.

¹ Zie ook: www.digitaleoverheid.nl/dossiers/wet-digitale-overheid/

De routeervoorziening is weliswaar een nieuw element, maar de inspanning om erop aan te sluiten is vergelijkbaar met de aansluiting op de al bestaande inlogmiddelen en zal daarmee de facto de bestaande werkwijzen blijven faciliteren. Of zelfs verminderen omdat één aansluiting op de routeervoorziening volstaat.

Het loggen van het gebruik van digitale diensten is voor veel bestuursorganen een nieuwe verplichting. Een aantal bestuursorganen geven aan dit nu nog niet te doen vanuit privacy overwegingen en/of overwegingen van systeempowerformance. De Wdo stelt nadere regels over het loggen van de (persoons)gegevens over het gebruik van digitale diensten en stelt dit verplicht.

De Wdo legt de verplichtingen met betrekking tot het identificatiestelsel voor waterschappen, provincies en hun samenwerkingsverbanden vast. Er is daarmee geen vrijblijvendheid en eigenstandige afweging meer mogelijk in de aansluiting en gebruik van de componenten van het identificatiestelsel. Bestuursorganen die op dit moment bijvoorbeeld nog niet zijn aangesloten op DigiD omdat ze niet tot nauwelijks diensten aan natuurlijke personen leveren, die een substantieel of hoog beveiligingsniveau vereisen, hebben straks die vrijheid niet meer.

Het bestuur zal zich moeten verantwoorden over de naleving van de Wdo. Provincies zullen zich moeten verantwoorden aan het Rijk en waterschappen (en gemeenten) zullen zich moeten verantwoorden aan provincies. In de huidige situatie hoeven bestuursorganen zich niet te verantwoorden over onderdelen van de Wdo. Op dit moment is het nog niet bekend welke Informatieverplichtingen voor bestuursorganen aan de naastgelegen overheidslaag uit de Wdo voortvloeien.

Vraag 3: Wat betekenen deze veranderingen voor de organisatie? Denk hierbij aan technische aanpassingen, aanpassingen in beleid, werkproces, juridische zaken en informatieondersteuning.

De nu voorliggende tranche regels van de Wdo stellen een aantal directe eisen aan waterschappen en provincies. Onderstaande tabel geeft een samenvatting van deze vereisten en de directe acties die bestuursorganen daarop moeten nemen. In hoofdstuk 3 zijn de nadere details opgenomen:

Regelgeving	Vereisten	Acties Bestuursorganen:
Besluit beveiligde verbindingen	Alle websites van bestuursorganen voldoen aan een minimale set algemene geaccepteerde veiligheidstandaarden.	- moeten inventariseren welke websites onder hun beheer vallen; - moeten verifiëren of de vereiste veiligheidstandaarden correct zijn geïmplementeerd.
Besluit digitale overheid	- Toegang tot elektronische dienstverlening is afdoende beveiligd - Gebruik van de digitale dienstverlening wordt gelogd.	- treffen maatregelen voor een informatieveilige toegang tot elektronische diensten; - regelen het loggen van het gebruik van elektronische diensten.
Regeling aansluitingschema	Bestuursorganen voldoen aan de acceptatieplicht van toegelaten en erkende inlogmiddelen door aan te sluiten op de componenten van de Wdo. Aansluiting en ingangsdatum van de acceptatieplicht gaat in op een zelf te bepalen datum.	- voeren een impactanalyse uit en bepalen hun uitgangssituatie; - stellen een aansluitingsplan op en stellen vast wanneer ze op welke component kunnen aansluiten; - ze rapporteren de voorgenomen aansluitdata aan de minister; - richten hun websites voor digitale diensten zo in dat diensten ook aan gemachtigden zijn te leveren; - en voeren het aansluitplan uit.
Regeling betrouwbaarheidsniveau	Van alle elektronische diensten is vastgesteld welke betrouwbaarheidsniveau noodzakelijk is gegeven de aard van de gegevens die voor die dienst worden uitgewisseld.	- stellen vast welke diensten elektronisch worden verleend; - bepalen per dienst de aard van de gegevens die voor die dienst worden uitgewisseld; - stellen per dienst vanuit een risicoperspectief vast welk betrouwbaarheidsniveau voor de inlogmiddelen bij de desbetreffende dienst passend is.

De Wdo vereist dan ook een samenhangende aanpak door verschillende specialisten op het gebied van ICT, Dienstverlening, Juridisch, Privacy en Informatieveiligheid. Deze activiteiten moeten in samenhang uitgevoerd worden zodat het bestuursorgaan op de door haar genoemde datum in de regeling aansluitschema, kan voldoen aan de acceptatieplicht van de Wdo. Daarbij komt dan Wdo niet alleen staat (zie ook paragraaf 3.2). Er zijn meerdere wetten met betrekking tot de digitale overheid die nu actueel zijn. Deze wetten kennen raakvlakken en vereisen veelal gelijksoortige expertises. Daarom is het verstandig de invoering van al deze wetten in één team onder te brengen, zo kunnen zij de invoering van de verschillende wetten onderling goed prioriteren en de opgedane kennis en ervaring met impactanalyses en aansluittrajecten steeds hergebruiken.

Aanbeveling

Binnen organisaties moet gezorgd worden voor een afgestemde multidisciplinaire aanpak, waarbij expertise nodig is op het gebied van dienstverlening, juridisch, ICT, informatieveiligheid en privacy. De Wdo beslaat dermate veel expertisegebieden dat deze verbinding vereist is. Omdat de Wdo niet op zich zelf staat is het verstandig de invoering van de verschillen wetten met betrekking tot de digitale overheid bij één team in de organisatie onder te brengen.

Aanbeveling

In algemene zin betekent de Wdo voor het bestuur met name dat zij de organisatie de ruimte moet geven om aan de verplichtingen te voldoen. Daarnaast zal er een besluit nodig zijn om het betrouwbaarheidsniveau vast te stellen, waarop het bestuursorgaan haar digitale diensten aanbiedt. Tot slot willen we de besturen van provincies en waterschappen in overweging geven voor de wettelijke verplichtingen op het gebied van digitalisering een duidelijke portefeuillehouder aan te wijzen op bestuurlijk niveau. Digitalisering is al lang niet meer alleen van de bedrijfsvoering, maar is in toenemende mate het dominante kanaal voor contact met inwoners en ondernemers. Het is van belang dat dit contact veilig, effectief en efficiënt tot stand komt. En volgens de afspraken die daar binnen de overheid over zijn gemaakt en die zijn vastgelegd in wet- en regelgeving (onder meer de Wdo). Wat ons betreft bij uitstek een bestuurlijke aangelegenheid.

Informatieverplichtingen

Het bestuur zal de naastgelegen overheidslaag moeten informeren over de naleving van de Wdo. Dit betekent logischerwijs dan ook dat het bestuur informatie moet verzamelen over de invoering van de Wdo. Op dit moment is de scope, het detailniveau en de beoogde frequentie van deze rapportages nog niet bekend.

Interbestuurlijk toezicht van provincies

Het interbestuurlijk toezicht zoals dat nu voorligt in de Wdo is voor provincies niet uitvoerbaar. Daarvoor is nadere uitwerking nodig.

- In de eerste plaats is nog veel niet voldoende gedefinieerd (zoals bijvoorbeeld de informatieverplichting, zie vorige punt).
- Het roept fundamentele vragen op over hoe de specifieke toezichtbepalingen van de Wdo zich (staatsrechtelijk) verhouden tot het generieke interbestuurlijke toezicht van provincies.
- De Wdo reikt de provincies geen aanvullende instrumenten aan om naleving te bevorderen. En de vraag is of de bestaande generieke instrumenten voor de Wdo passend en toereikend zijn. Dit introduceert een afbreukrisico voor gedeputeerde staten als toezichthouder op gemeenten en waterschappen.
- De Wdo vereist capaciteit van specialisten op het gebied van informatiebeveiliging, privacy, dienstverlening, juridische zaken en ICT. Deze kennis is in huis maar is ingezet voor de eigen bedrijfsvoering.

Vraag 4: Wat betekenen deze veranderingen voor het bestuur? In het bijzonder de uitoefening van het interbestuurlijk toezicht op informatieveiligheid en naleving van verplichte standaarden door provincies op en de opvolging hiervan bij gemeenten en waterschappen en hun uitvoeringsorganisaties.

Algemeen

Nationaal maar ook vanuit Europees verband komt er steeds meer wetgeving op digitaal gebied af op bestuursorganen. De wet digitale overheid is daar slechts één van. Deze wetten hangen vaak samen en grijpen op elkaar in. In de praktijk is de verantwoordelijkheid voor dergelijke wettelijke verplichtingen vaak niet voldoende helder belegd.

- Voor waterschappen is het wenselijk dat het toezicht op de Wdo in alle provincies op een soortgelijke manier wordt ingericht. Waterschappen hebben vaak met meer dan één provincie te maken hebben. Zo ligt het werkgebied van Rivierenland in vijf verschillende provincies. De waterschappen geven hierbij de wens aan dat bij de uniforme verplichtingen van de Wdo ook een uniform toezichtskader past². Dit strookt echter niet met de decentrale opzet van het toezicht in de Wdo. De omvang van de provincies is zo verschillend dat elke provincie het toezicht op maat heeft vormgegeven.

Vraag 5: Zijn de provincies, waterschappen en hun samenwerkingsverbanden voldoende toegerust voor een doeltreffende uitvoering?

Provincies, waterschappen en hun samenwerkingsverbanden zijn in beginsel in voldoende mate toegerust om uitvoering te geven aan de verplichtingen van de Wdo. De benodigde expertise op het gebied van dienstverlening, juridisch, privacy, ICT en informatieveiligheid is aanwezig. Daar zijn echter wel een aantal kanttekeningen bij te plaatsen.

- De kennis over de Wdo is nog maar beperkt aanwezig (zoals blijkt uit de survey). Daarbij komt dat op onderdelen de verplichtingen nog niet voldoende duidelijk zijn. Bestuursorganen zullen zich de komende tijd in de Wdo moeten verdiepen.
- De Wdo betekent dat er binnen de reguliere taken op het gebied van privacy, dienstverlening, juridische zaken, ICT en informatieveiligheid werkzaamheden bijkomen en de eisen zijn verplichtender van karakter. Daarbij geldt dat de Wdo niet op zichzelf staat. Er is veel gerelateerde en aanpalende wetgeving (zie paragraaf 3.2) die op dezelfde capaciteit een beroep doet. In onze ervaring is op deze functies de capaciteit in provincies en waterschappen niet altijd ruim bemeten (hoewel dat natuurlijk per organisatie verschilt). Het risico bestaat dan ook dat de uitvoering van de Wdo en gerelateerde wetten in de knel komt.
- De Wdo vergt coördinatie en samenwerking op landelijk niveau. Zo is het bijvoorbeeld in de 'ontwerpfase', wenselijk als de classificatie van de betrouwbaarheidsniveau af te stemmen. Vanuit het perspectief van de burger is het niet wenselijk als er teveel verschillen tussen bestuursorganen zijn.

Dit geldt ook voor de beheerfase, zo zullen bijvoorbeeld door technische ontwikkelingen de voorgeschreven standaarden in het besluit beveiligde verbindingen, kunnen veranderen. Dit moet gemonitord en opgevolgd worden. Volgens ons is het efficiënter om dit landelijk te organiseren dan dat ieder bestuursorgaan dit voor zichzelf doet. Waterschappen hebben dergelijke landelijke coördinatie via het UvW, Waterschapshuis en het CERT watermanagement op dit vlak al structureel georganiseerd. Dit geldt in mindere mate voor provincies. Zij hebben dit georganiseerd in IDA verband, maar dat is een tijdelijk programma.

Aanbeveling

Op diverse onderdelen van de Wdo is nog sprake van veel onbekendheid. Bestuursorganen zullen zich de komende tijd in de Wdo moeten verdiepen. Daarnaast vergt de Wdo coördinatie en samenwerking op landelijk niveau, zowel in de ontwikkel- als de beheerfase.

Vraag 6: Hoe kunnen veranderingen succesvol worden geïmplementeerd? Welke activiteiten zijn nodig, hoe zijn die het beste te faseren en wat zijn de randvoorwaarden en risico's?

Aanbeveling

Voor een succesvolle invoering van de Wdo is het van belang dat de implementatie in samenhang projectmatig wordt opgepakt. Daarbij hebben het ministerie van BZK, IPO/UvW en individuele waterschappen en provincies een rol te vervullen. Hieronder geven we per betrokken bestuurslaag de te zetten stappen.

Ministerie van BZK

- Wij denken dat het van belang is de Wdo op onderdelen te verhelderen en nader te specificeren. Zo roepen de bepalingen over informatieveiligheid nog vragen op, is nog niet voldoende duidelijk welke gegevens over het gebruik van elektronische diensten gelogd moeten worden (bijv. wat zijn systeemtechnische gegevens?) en zijn de informatieverplichtingen over de naleving van de Wdo en de vormgeving van het toezicht nog niet bekend. Idealiter wordt deze verheldering en nadere specificatie in goed overleg met de verschillende overheidslagen vormgegeven, zodat het aansluit bij de informatiebehoefte en de uitvoerbaarheid geborgd is. Ook zijn de kosten en de wijze van dekking van de centrale componenten van het identificatiestelsel nog niet bekend.

² Een coördinerend bestuursorgaan zou kunnen optreden conform een coördinatiebesluit op grond van paragraaf 3.5.3 van de Awb; dit is echter niet in de Wdo voorgeschreven.

- Voor de besluitvorming en planning over invoering van de Wdo door provincies en waterschappen is het van belang dat duidelijker wordt wanneer de verschillende onderdelen van de Wdo beschikbaar komen. Het gaat dan bijvoorbeeld om de ontsluiting van eHerkenning via de routeervoorziening en de beschikbaarheid van de machtingsvoorziening. Bestuursorganen kunnen dan beter bepalen welke aansluitroute voor hen het meest passend is en wanneer zij kunnen voldoen aan de acceptatieplicht.
- De Wdo bevat een aantal nieuwe elementen voor waterschappen en provincies, onder meer de routeervoorziening, de mogelijkheid van cluster aansluitingen en het BSN Koppelregister. Deels zijn er in andere sectoren al wel ervaringen met soortgelijke voorzieningen opgedaan. Deze ervaringen zouden vastgelegd kunnen worden in handreikingen en stappenplannen zodat meer zicht ontstaat op de benodigde stappen.
- Zoals gezegd zijn een aantal onderdelen van de Wdo nieuw voor waterschappen en provincies. Het is dan ook van belang om in de komende periode pilots uit te voeren om ervaring in de context van provincies, waterschappen en hun samenwerkingsverbanden op te doen, met aansluitingen op die onderdelen. Deze ervaringen kunnen dan ook landen in handreikingen en stappenplannen zodat alle waterschappen en provincies hiervan kunnen profiteren. Het ministerie en haar uitvoeringsdiensten kunnen deze pilots ondersteunen en faciliteren.

IPO en UvW

- Het IPO en de UvW zijn goed gepositioneerd om een centrale coördinerende rol bij de invoering van de Wdo te vervullen. Zij kunnen bijvoorbeeld de eerder genoemde pilots begeleiden en de communicatie en voorlichting over de resultaten voor hun rekening nemen.
- In de nadere verheldering van de vereisten van de Wdo kunnen IPO en UvW het belang van provincies, waterschappen en hun uitvoeringsorganisaties inbrengen. We denken daarbij met name aan de nadere vormgeving van het interbestuurlijk toezicht op de Wdo.
- IPO en UvW kunnen ook een rol spelen in het gecoördineerd vaststellen van de betrouwbaarheidsniveaus zodat voor soortgelijke diensten bij alle provincies en waterschappen soortgelijke betrouwbaarheidsniveaus worden gehanteerd. Voor de waterschappen zou het programma informatieveiligheid en privacy van het Waterschapshuis daarin een rol kunnen spelen om de uniforme uitvoering te waarborgen.
- Ook na invoering van de Wdo zien wij een rol voor UvW en IPO. Onderdelen van de Wdo zullen wijzigen. Door technische ontwikkelingen zullen er bijvoorbeeld nieuwe versies van standaarden en richtlijnen nodig zijn. Het is ons inziens efficiënt om dit centraal te coördineren zodat niet ieder bestuursorgaan zelf de ontwikkelingen in de gaten hoeft te houden.
- Voor de waterschappen geldt dat zij in het Waterschapshuis beschikken over een uitvoeringsorganisatie met specifieke digitaliseringsexpertise. Zij kunnen dan ook gedurende de invoering van de Wdo maar ook gedurende het beheer een centrale en coördinerende rol vervullen, zij beschikken daarbij immers over de benodigde kennis.

Provincies, waterschappen en hun uitvoeringsorganisaties

Het echte werk voor de invoering van de Wdo zal door provincies, waterschappen en uitvoeringsorganisaties zelf gedaan moeten worden. Het is ons inziens van belang dat dit projectmatig met een multidisciplinair team wordt opgepakt. Expertise op het gebied van ICT, informatieveiligheid, privacy, juridische zaken en dienstverlening zijn in een dergelijk team nodig. We zien daarbij de volgende stappen:

- **Bestuurlijke opdracht.** Het bestuur zal een duidelijke opdracht aan de organisatie moeten geven om de Wdo in te voeren. Bij voorkeur wordt deze opdracht belegd bij de portefeuillehouder die ook andere wettelijke verplichtingen zoals de Wmebv en SDG in zijn of haar portefeuille heeft. Zo is de invoering in samenhang van deze wetten geborgd.
- **Impactanalyse.** Elke organisatie kent zijn eigen uitgangspositie. Het is dan ook van belang om, mede op basis van deze rapportage en andere beschikbare informatie, de impact op de eigen organisatie te bepalen, evenals de meest passende aanvliegroete en dit in een projectplan vast te leggen.
- **Realisatie.** Op basis van het projectplan kunnen dan de benodigde werkzaamheden uitgevoerd worden.
 - Digitale diensten moeten geclassificeerd worden;
 - Betrouwbaarheidsniveaus moeten geconfigureerd worden;
 - Veiligheidsstandaarden moeten worden geconfigureerd;
 - Beheersing van informatieveiligheid moet op niveau worden gebracht;
 - Aansluitingen op de componenten moeten gerealiseerd worden;
 - Websites moeten het gebruik van machtigingen faciliteren;
 - Logging van gegevens moet worden gerealiseerd.

- **Inregelen informatievoorziening.** Op basis van de nog vast te stellen informatieverplichtingen zullen bestuursorganen de informatievoorziening over de naleving van de Wdo in dienen te regelen.
- **Vormgeven toezicht.** Provincies zullen het toezicht op de Wdo moeten inbedden in hun regulier generieke toezicht. Randvoorwaardelijk is daarbij wel dat er meer duidelijkheid vanuit de minister komt over de vormgeving van het toezicht.
- **Inregelen beheer.** Bestuursorganen zullen het beheer en onderhoud van de voorzieningen van de Wdo moeten regelen. Met name het loggen vergt daarbij structurele inspanningen.

Fasering

In onderstaande tabel is in hoofdlijnen een mogelijke fasering voor de invoering van de Wdo weergegeven. Het spreekt voor zich dat een dergelijke fasering nog sterk afhangt van de te maken afspraken. Leidend voor de fasering zijn immers de afspraken die de individuele bestuursorganen zullen vastleggen in het aansluitschema. Niet iedereen zal daarbij hetzelfde tempo hebben. Deze fasering is dan ook vooral bedoeld om een indruk te geven hoe het zou kunnen verlopen. Uitgangspunt voor deze inschatting van de doorlooptijd is een voorziene inwerkingtreding van de Wdo op 1 juli 2022. In dit overzicht zijn de voorgaand beschreven stappen in de tijd uitgezet.

Jaar	2021		2022				2023				2024
Kwartaal	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	e.v.
BZK											
Verhelderen vereisten, planning en kosten											
Inwerkingtreding Wdo					1 juli						
IPO/UvW											
Begeleiden pilots											
Inventariseren aansluitdata											
Communiceren en voorlichten											
Coördineren beheer en onderhoud											
Provincies en waterschappen											
Impactanalyse											
Realiseren											
Informatievoorziening inregelen											
Beheren en onderhouden											
Provincies											
Ontwikkelen toezichtskader Wdo											
Inbedden toezicht											
Toezicht uitvoeren											

Randvoorwaarden en risico's

Voor de succesvolle invoering zien we vanuit het perspectief van provincies en waterschappen de volgende belangrijkste randvoorwaarden:

Beschikbare middelen: Het is van belang dat voor invoering van de wet voldoende middelen beschikbaar komen. Voor het IPO en UvW geldt dat er middelen nodig zijn om pilots te begeleiden, resultaten daarvan vast te leggen en te ontsluiten voor provincies, waterschappen en hun samenwerkingsverbanden. Ook zullen er structurele middelen nodig zijn voor de beheerfase, indien besloten wordt dit centraal te coördineren.

Voor individuele bestuursorganen geldt dat er incidentele middelen nodig zijn voor de projectmatige invoering en structurele middelen om het beheer vorm te geven.

Risico: Zonder adequate middelen komt de invoering van de Wdo niet tot stand. De werkzaamheden zijn daarvoor naar onze inschatting te omvangrijk om binnen de reguliere taakuitoefening te realiseren.

Goede bestuurlijke en organisatorische verankering:

De ervaring leert dat duidelijk bestuurlijk opdrachtgeverschap helpt focus aan te brengen en de benodigde prioriteit te verkrijgen binnen de organisatie. We denken dat bestuurlijk opdrachtgeverschap voor de invoering van de Wdo noodzakelijk is vanwege de samenhang met andere wettelijke verplichtingen en vanuit compliancy overwegingen.

Risico: zonder duidelijk opdrachtgeverschap zal de invoering van de Wdo onvoldoende aandacht en prioriteit binnen de organisatie krijgen.

Duidelijkheid over de planning, vereisten en kosten:

Het is van belang tijdig duidelijkheid te krijgen over de planning van de centrale componenten (bv. de ontsluiting van eHerkenning via de routevoorziening, de beschikbaarheid van het machtigingenregister). Dat faciliteert een efficiënte invoering. Ook is het van belang duidelijkheid op de eerder genoemde onderdelen van de wet te geven en uit te werken. Dan kunnen bestuursorganen een passende strategie vaststellen en doeltreffend de Wdo invoeren.

Risico: Onvoldoende duidelijkheid over planning, vereisten en kosten van de wet leidt er toe dat bestuursorganen niet tot besluitvorming kunnen overgaan. Dat zal leiden tot vertraging bij de invoering van de Wdo.

Vraag 7: Welke eenmalige en structurele kosten en besparingen zijn aan deze nieuwe regelgeving verbonden?

De volgende kosten voor de invoering van de Wdo zijn te onderscheiden:

- **De kosten voor de centrale onderdelen van de infrastructuur.** De minister zal deze doorbelasten. De omvang van deze kosten en de wijze waarop de doorbelasting plaats zal vinden, zijn op dit moment niet bekend.
- **De kosten voor de invoering van de Wdo.** Deze hangen af van de uitgangssituatie van de organisatie in kwestie. Voor het gemiddelde waterschap of provincie betekent dit dat zij kosten moeten maken om aan te sluiten op de nieuwe elementen van de Wdo. Daarnaast geldt dat vrijwel nog geen enkel waterschap en provincie aangesloten zijn op DigiD machtigen. Bestuursorganen zullen dan ook kosten maken om aan te sluiten op het nog te realiseren machtigingsregister en kosten moeten maken om de digitale dienstverlening zo in te richten dat diensten ook aan een gemachtigde te leveren zijn. Bestuursorganen die zijn achtergebleven zullen meer kosten moeten maken om het been bij te trekken.
- **De kosten voor het beheer en onderhoud van de onderdelen van de Wdo.** Daarbij springt met name logging er uit als een element dat structurele beheerlasten veroorzaakt.
- **De kosten voor de informatieverplichtingen aan de minister.** Bestuursorganen zullen de naastgelegen overheidslaag moeten informeren over de naleving van de Wdo. Dit brengt administratieve lasten met zich mee. Er is op dit moment nog niet bekend wat deze informatieverplichtingen zijn.
- **De kosten voor het toezicht van provincies.** Provincies zullen kosten moeten maken voor de inzet van specialisten voor de opvolging van het toezicht op de Wdo. Voor provincies is het toezicht op de Wdo een nieuwe taak in een nieuw beleidsterrein³. Het is dan ook van belang goede afspraken met de minister te maken over de bekostiging van de benodigde capaciteit. Hoe omvangrijk deze nieuwe taak is, is op dit moment nog lastig te bepalen.

³ Weliswaar hebben de provincies nu een taak op het gebied van informatiebeheer en houden zij toezicht op de archiefwet, maar dat is wat ons betreft wezenlijk anders van karakter.

Overall conclusies

Als we vanuit onze professionele expertise kijken, naar hetgeen dat al is bepaald in de Wdo, komen we tot ons volgende oordeel:

- In beginsel is de Wdo voor provincies en waterschappen naar onze mening in voldoende mate uitvoerbaar, er zijn naar onze mening geen overkomelijke belemmeringen. Waterschappen en provincies leveren relatief weinig diensten aan burgers (op waterschappen die zelf belasting innen na). En bij de diensten die wel worden geleverd worden relatief weinig vertrouwelijke gegevens uitgewisseld. De impact is daarmee relatief beperkt, in de zin dat het geen grote veranderingen in de organisatie vereist.
- Qua toerusting van provincies en waterschappen zien we wel een risico. De Wdo noodzaakt dat alle digitale diensten opnieuw tegen het licht worden gehouden. En dat is een stevige inspanning. Er zal behoorlijk moeten worden geïnvesteerd (zowel in mensen als middelen) om aan alle eisen uit de wet te kunnen voldoen. De beschikbare capaciteit op de relevante expertises (dienstverlening, ICT, Juridisch, Informatieveiligheid en privacy) is in veel provincies en waterschappen niet heel groot (hoewel dit per organisatie kan verschillen). Daarbij komt dat de Wdo niet de enige verplichting is die een beroep op deze experts doet. Er is bij diverse wetgevingstrajecten sprake van vertraging of uitstel. Dat leidt mogelijk tot een stapeling van wetten die allemaal in 2022 in werking gaan treden.
- Het is opvallend dat de Wdo veel 'losse eindjes' kent en op onderdelen nog niet voldoende duidelijk is wat nu precies van waterschappen en provincies wordt verwacht. Bestuursorganen noemen daarbij vaak logging en informatieveiligheid. We vinden dat een risico. Onduidelijkheid staat een efficiënte en effectieve invoering in de weg en kan tot vertraging leiden.
- De specifieke toezichtstaak (artikel 17 lid 3) voor provincies op de naleving van de Wdo is nu niet uitvoerbaar. Er is wat ons betreft nog niet voldoende duidelijk wat van provincies wordt verwacht en het lijkt niet voldoende doordacht hoe deze taak zich verhoudt tot de generieke toezichtstaak van provincies.

HOOFDSTUK 1

Inleiding

1.1 Context en achtergrond

De Nederlandse samenleving digitaliseert. Dit betekent dat steeds meer transacties digitaal plaatsvinden, ook met de overheid. Het is belangrijk om te zorgen dat dit veilig en overzichtelijk kan. Het wetsvoorstel Wet digitale overheid (Wdo) legt de basis voor deze digitalisering van de overheid (voorheen de Wet Generieke Digitale Infrastructuur (Wgdi)). De Wdo heeft als doel het regelen van veilig en betrouwbaar inloggen voor Nederlandse burgers en bedrijven bij de (semi) overheid.⁴

Het wetsvoorstel is een zogeheten kaderwet; de wet regelt algemene principes, verantwoordelijkheden en procedures, maar geen gedetailleerde regels.⁵ De uitwerking van de Wdo vindt plaats in de lagere regelgeving, zoals in algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen. Zo is er ruimte voor innovatie, verdere keuzes en nieuwe voorzieningen en functionaliteiten. De wet zorgt zo voor flexibiliteit bij nieuwe ontwikkelingen, maar ook dat belangrijke waarden en zekerheden voor burgers zoals gebruikersvriendelijkheid, betrouwbaarheid, veiligheid, privacy en digitale inclusie altijd geborgd zijn. Deze wet:⁶

- legt de taken en verantwoordelijkheden vast voor veilige toegang tot de digitale overheid;
- legt verplichtingen op aan medeoverheden om veilig en betrouwbaar aan te sluiten, en hun dienstverlening in te delen op een betrouwbaarheidsniveau;
- stelt regels over de bekostiging daarvoor;
- biedt zekerheden voor burgers en bedrijven;
- biedt uitgangspunten voor informatiebeveiliging en de verwerking van persoonsgegevens.

Uit eerdere uitvoeringstoetsen in 2017 van de Wgdi is gebleken dat onvoldoende bekend was over kosten, planning en technische eisen. Destijds is dan ook geadviseerd om opnieuw een uitvoeringstoets uit te voeren op het moment dat deze informatie beschikbaar is. Dat moment is nu aangebroken. VNG Realisatie doet ook een uitvoeringstoets op de wet. Provincies en waterschappen hebben besloten om de uitvoeringstoets in gezamenlijkheid te laten uitvoeren.

1.2 Reikwijdte van uw vraag aan Berenschot

Het Interprovinciaal Overleg (IPO) en de Unie van Waterschappen (UvW) hebben Berenschot gevraagd om een uitvoeringstoets op de nu voorliggende nadere regelgeving uit te voeren. De scope van uitvoeringstoets is de nu voorliggende nadere regelgeving in het kader van de Wdo, zijnde:

- Het besluit beveiligde verbindingen
- Het besluit digitale overheid
- De regeling betrouwbaarheidsniveaus
- De regeling aansluitschema

Gedurende het onderzoek is de Wdo en de nadere regelgeving in de eerste kamer behandeld. Naar aanleiding daarvan heeft de minister toegezegd met een novelle te komen, waarin de beginselen 'open source', 'privacy by design' en een verbod op het verhandelen van gegevens zijn verankerd.

Daarnaast is gevraagd om voor zover als mogelijk de gevolgen over het aankomende besluit en de regeling basisvoorziening machtigen en de regeling bekostiging uit te voeren. Aanvullend zijn uiteraard de relevante bepalingen uit de Wdo met betrekking tot deze nadere regelgeving meegenomen, met name de bepalingen ten aanzien van naleving uit de Wdo. Buiten scope valt het tijdelijk besluit digitale toegankelijkheid.

⁴ Zie ook: www.digitaleoverheid.nl/dossiers/wet-digitale-overheid/

⁵ Ibid.

⁶ Ibid.

Dit besluit zal ook onder de Wdo vallen, maar dit besluit is inmiddels al in werking getreden.

Tot slot heeft u verzocht niet alleen de gevolgen voor de waterschappen en de provincies te onderzoeken, maar ook haar samenwerkingsverbanden en dan met name regionale belastingkantoren en de omgevingsdiensten.

1.3 Onderzoeksvragen

De waterschappen en provincies hebben behoefte aan inzicht in de impact en uitvoerbaarheid van de Wdo. Vanuit ervaringen uit het verleden en de reeds gestarte uitvoeringstoets door VNG Realisatie, blijkt een uitvoeringstoets hiervoor het geëigende middel. In deze rapportage geven we antwoord op de volgende vragen:

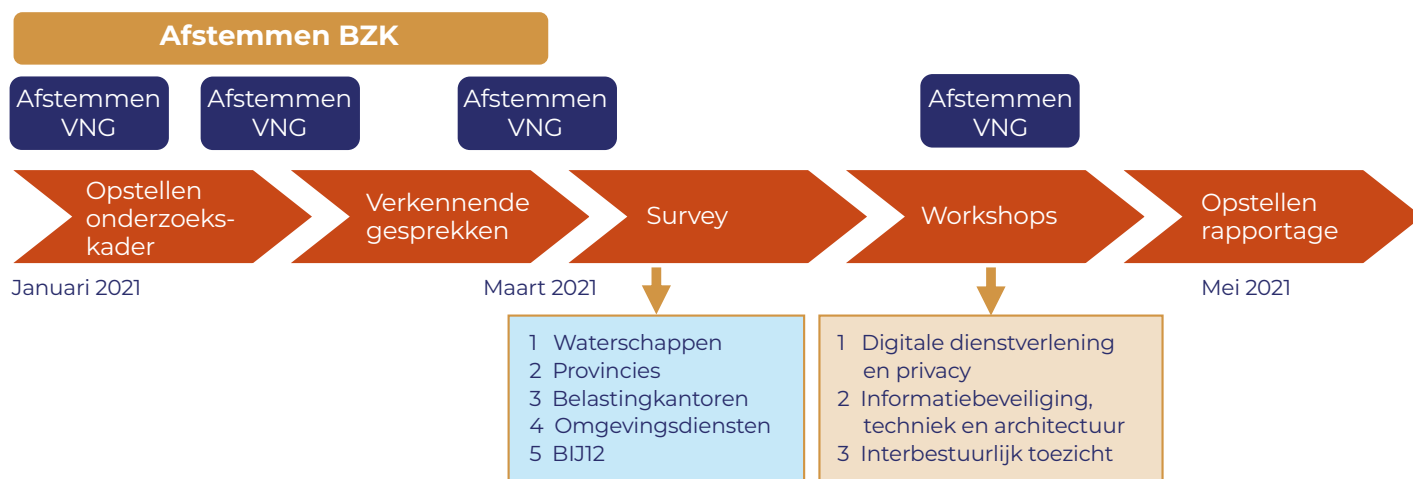
- Wat wijzigt er door de nieuwe regelgeving in de verplichtingen en werkwijze van de waterschappen, provincies en hun samenwerkingsverbanden?
- Wat betekenen deze veranderingen voor de organisatie? Denk hierbij aan technische aanpassingen, aanpassingen in beleid, werkproces, juridische zaken en informatieondersteuning.
- Wat betekenen deze veranderingen voor het bestuur? In het bijzonder de uitoefening van het interbestuurlijk toezicht op informatieveiligheid en naleving van verplichte standaarden door provincies op en de opvolging hiervan bij gemeenten en waterschappen.
- Zijn de provincies, waterschappen en hun samenwerkingsverbanden voldoende toegerust voor een doeltreffende uitvoering?
- Hoe kunnen veranderingen succesvol worden geïmplementeerd? Welke activiteiten zijn nodig, hoe zijn die het beste te faseren en wat zijn de randvoorwaarden en risico's?
- Welke eenmalige en structurele kosten en besparingen zijn aan deze nieuwe regelgeving verbonden?

1.4 Leeswijzer

De samenvattende conclusies en aanbevelingen die u hiervoor heeft kunnen lezen geven het overzicht van onze bevindingen. In hoofdstuk 2 geven we inzicht op welke wijze we tot onze bevindingen zijn gekomen. In hoofdstuk 3 is onze analyse opgenomen van de beschikbare documentatie waaronder de diverse besluiten, wetten en regelingen. Tot slot is in hoofdstuk 4 de inventarisatie van de impact weergegeven zoals we die middels enquêtes, gesprekken en workshops hebben opgehaald.

HOOFDSTUK 2

Onderzoeksopzet



Figuur 1. **Onderzoeksplan en activiteiten op hoofdlijnen weergegeven in de tijd**

2.1 Methode en opzet van het onderzoek

Om de impact en uitvoerbaarheid van de Wdo te kunnen bepalen hebben we gebruik gemaakt van verschillende onderzoeksmethodieken, te weten: een juridische analyse, verkennende interviews, een survey en workshops. In onderstaande figuur is onze aanpak in hoofdlijnen weergegeven.

We zijn begonnen met de juridische analyse van de wetsteksten, besluiten en regelingen en hebben dit gepresenteerd in een onderzoekskader. Vervolgens hebben we een viertal verkennende gesprekken gevoerd met waterschappen en provincies om een eerste inventarisatie van de impact te kunnen maken. Vervolgens hebben we een survey uitgezet bij alle provincies, waterschappen, belastingkantoren, omgevingsdiensten en BIJ12. De survey had betrekking op alle onderwerpen, behalve het interbestuurlijk toezicht. Het interbestuurlijk toezicht hebben we in separate gesprekken en workshops onderzocht, omdat deze taak specifiek belegd is bij provincies. De resultaten van de survey hebben we gevalideerd en verdiept tijdens vier workshops. We hebben dezelfde vragenlijsten voor provincies, waterschappen, belastingkantoren en omgevingsdiensten gebruikt en gezamenlijke (gemengde) workshops georganiseerd.

Ten slotte hebben we een conceptrapportage opgesteld die we hebben voorgelegd aan de begeleidingsgroep van het IPO en de UvW én een aantal betrokkenen vanuit provincies en waterschappen. Deze concept rapportage hebben we uiteindelijk verwerkt tot een definitief eindrapport.

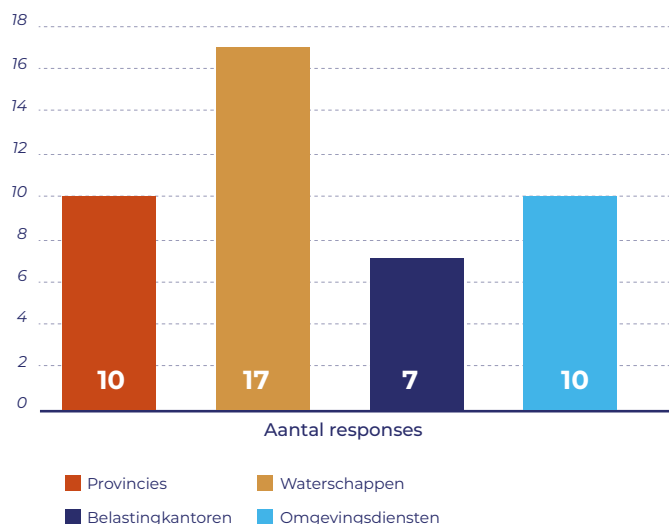
Gedurende het onderzoek hebben we meermaals afgestemd met BZK. Zo zijn we zowel mondeling als schriftelijk in gesprek geweest over vragen en onduidelijkheden en hebben we het onderzoekskader getoetst. Daarnaast hebben we meermaals afgestemd met de VNG, die gelijktijdig bezig was met een uitvoeringstoets voor de gemeenten. Met de VNG is het onderzoekskader en de voortgang besproken.

2.2 Survey en workshops

2.2.1 Survey

De survey is uitgezet bij alle provincies, waterschappen, omgevingsdiensten, belastingkantoren en BIJ12. Van BIJ12 hebben we geen respons ontvangen. In de volgende grafiek is het totale aantal responses per bestuursorgaan weergegeven (N=44). Het was in de vragenlijst niet verplicht om alle vragen te beantwoorden.

Om die reden geven we bij de presentatie van de survey resultaten in hoofdstuk 4 per vraag aan (met de aanduiding N) door hoeveel respondenten de vraag is beantwoord.



Figuur 2. Totaal aantal responses per bestuursorgaan

2.2.2 Workshops

We hebben in totaal vier workshops georganiseerd om de survey resultaten te valideren en te verdiepen. We hebben twee workshops rondom digitale dienstverlening en privacy en twee workshops rondom informatiebeveiliging en ICT georganiseerd. In deze workshops zijn de volgende onderwerpen aan bod gekomen:

- Workshop digitale dienstverlening en privacy
 - Inlogmiddelen
 - Routeervoorziening
 - Betrouwbaarheidsniveaus
- Workshop informatiebeveiliging en ICT
 - Inlogmiddelen
 - Beveiligde verbindingen
 - Logging
 - Informatiebeveiliging

Daarnaast hebben we een tweetal workshops rondom het interbestuurlijk toezicht (IBT) georganiseerd. Hierbij waren diverse vertegenwoordigers rondom IBT van provincies aanwezig, evenals een aantal mensen van VNG en waterschappen. Hierbij zijn de volgende onderwerpen aan bod gekomen:

- Het mogelijke toezichtsproces van provincies;
- De benodigde informatie voor het vormgeven van het toezicht;
- De benodigde inspanning van gemeenten, waterschappen en provincies om het toezicht vorm te geven.

2.3 Geconsulteerde functionarissen

In de gesprekken en workshops hebben we informatie opgehaald bij verschillende doelgroepen binnen provincies, waterschappen, omgevingsdiensten en regionale belastingkantoren. We hebben de volgende indeling naar doelgroepen gemaakt:

- **Informatiebeveiliging en privacy.** Tot deze doelgroep behoren CISO's en functionarissen gegevensbescherming van provincies, waterschappen, omgevingsdiensten en regionale belastingkantoren. Bij hen hebben we vooral informatie met betrekking tot de beveiligingsstandaarden en de consequenties voor de verwerking van persoonsgegevens opgehaald.
- **ICT en techniek.** Tot deze doelgroep behoren afdelingshoofden ICT die goed kunnen aangeven op welke voorzieningen hun organisatie is aangesloten en wat zij nog moeten doen om te voldoen aan de vereisten van de Wet digitale overheid en wat daarvoor een reële planning is.
- **Dienstverlening.** Tot deze doelgroep behoren verantwoordelijken voor (digitale) dienstverlening. Bij hen hebben we de consequenties voor de dienstverlening en benodigde informatie over de classificatie van de diensten opgehaald.
- **Interbestuurlijk toezicht (alleen provincies).** Hier hebben we ons gericht tot de verantwoordelijken van de provincies voor interbestuurlijk toezicht. Bij hen hebben we informatie opgehaald over de vormgeving van het interbestuurlijk toezicht op de Wdo.

HOOFDSTUK 3

Veranderingen Wdo en juridische analyse

3.1 Wet digitale overheid

De Wet digitale overheid regelt de toegang voor inwoners en ondernemers tot de digitale overheid in de Europese Unie. Daartoe ligt nu een aantal samenhangende besluiten en regelingen voor die handen en voeten geven aan de uitvoering van de Wet digitale overheid:

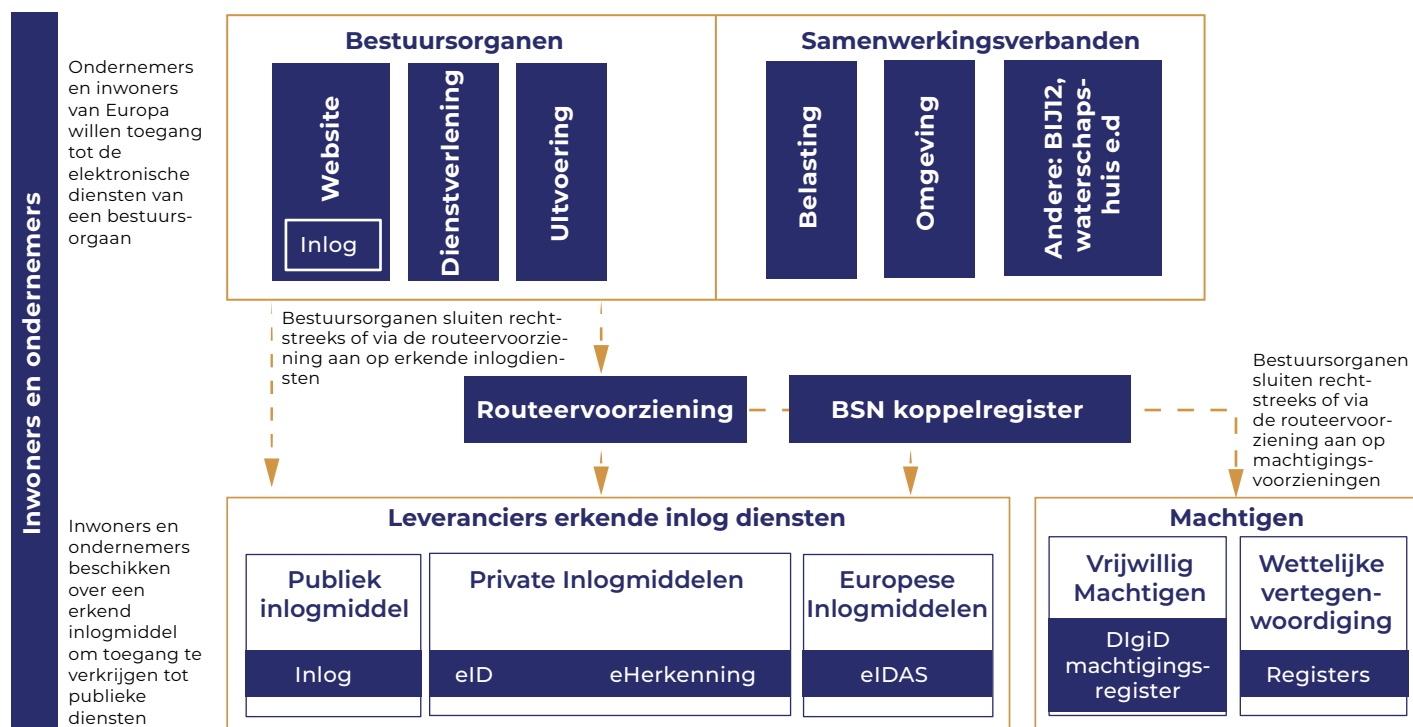
1. Het besluit digitale overheid stelt regels inzake de informatieveiligheid en de verwerking van persoonsgegevens die gebruikt worden in het kader van toegang tot elektronische dienstverlening.
2. Het 'besluit beveiligde verbindingen' regelt de verplichte toepassing van beveiligingsstandaarden voor overheidswebsites zoals die ook al langer op de 'pas toe en leg uit-lijst' van het forum van standaardisatie zijn opgenomen.
3. De 'regeling aansluitschema' faciliteert de gefaseerde invoering van Wet digitale overheid.
4. En de 'regeling betrouwbaarheidsniveaus dienstverlening' legt tot slot vast dat publieke dienstverleners bepalen welke beveiligingsniveaus nodig zijn voor hun verschillende producten en diensten. En de regeling biedt een schema waarmee deze classificatie kan worden uitgevoerd.

Daarnaast is het 'besluit basisvoorzieningen machtigen' en de 'regeling bekostiging' op komst. Deze waren op het moment van uitvoering van deze uitvoeringstoets nog niet gereed en vallen daarom buiten de scope van dit onderzoek.

Het is goed te beseffen dat de Wdo niet nieuw is. De Wdo reguleert en legt de ontwikkelingen rond identificatiemiddelen vast voor inwoners en ondernemers, zodat zij gebruik kunnen maken van de diensten van publieke dienstverleners. De Wdo bevat echter een paar elementen die verder gaan dan het huidige gebruik van DigiD, eIDAS en eHerkenning:

- De Wdo stelt regels voor de toelating van meerdere identificatiemiddelen. Via een open toelatingsproces kunnen straks (commerciële) leveranciers van identificatiemiddelen, indien zij aan de eisen voldoen, worden toegelaten tot het stelsel
- De Wdo stelt regels voor het gebruik van de routeervoorziening waarmee publieke dienstverleners ontzorgd kunnen worden. Door op de routeervoorziening aan te sluiten leggen zij verbinding met alle erkende en toegelaten identificatiemiddelen.
- De Wdo maakt het mogelijk het BSN versleuteld te verstrekken aan dienstverleners. Het BSN-koppelregister faciliteert de versleuteling en de ontcijfering van het BSN (voor daartoe gerechtigde organisaties) door het benodigde sleutelmateriaal ter beschikking te stellen.
- Tot slot maar niet in het minst legt de Wdo de verplichting op het gebruik van alle erkende en toegelaten identificatiemiddelen te accepteren.

In figuur 3 is de beoogde werking van het identificatiestelsel weergegeven.



Figuur 3. Globale structuur en werking van het identificatiesysteem

We lichten figuur 3 toe:

- Inwoners en ondernemers van Europa beschikken over een erkend privaat of publiek inlogmiddel.
- Met dit inlogmiddel kunnen ze toegang verkrijgen tot de elektronische dienstverlening van Nederlandse bestuursorganen.
- Bestuursorganen in Nederland bieden elektronische diensten aan via hun website. Dat kan variëren van een vergunning voor wateronttrekking, een aanvraag bijzonder transport over een provinciale weg of een kwijtschelding van de waterschapsbelasting.
- Sommige van deze diensten zijn alleen te leveren nadat de inwoner of ondernemer is ingelogd, zodat het bestuursorgaan de identiteit van de aanvrager kan vaststellen en kan vaststellen of de aanvrager bevoegd is om van de desbetreffende dienst of product gebruik te maken.
- Bestuursorgaan worden door de Wdo verplicht de erkende inlogmiddelen te accepteren voor de identificatie van de inwoner of ondernemer die van een dienst of product gebruik wil maken.
- Daartoe zullen bestuursorganen moeten aansluiten op de erkende inlogmiddelen. Dit kunnen ze rechtstreeks doen op de leveranciers van die erkende inlogmiddelen. Of via een routeervoorziening die de complexiteit van de verschillende inlogmiddelen voor het bestuursorgaan 'verbergt'. Op dit moment worden via de routeervoorziening alleen DigiD en eIDAS. Ontsluiting van eHerkenning en de andere inlogmiddelen en infrastructurele voorzieningen moet nog gerealiseerd worden.
- Het bestuursorgaan verkrijgt via het BSN koppelregister nadere identificerende persoonsgegevens van een inwoner (zoals het BSN nummer of de woonplaats) voor een verdere efficiënte afhandeling van de aanvraag of om vast te stellen of de desbetreffende aanvrager in aanmerking voor de desbetreffende dienst of product komt.
- Het bestuursorgaan zal daarnaast aansluiten op een machtigingsvoorziening. Dat is nu al mogelijk op DigiD machtigen voor vrijwillige machtiging. Op termijn zullen voor wettelijke vertegenwoordiging ook een aantal registers beschikbaar komen. Bestuursorganen zullen hierop kunnen aansluiten zodat ook wettelijke vertegenwoordigers als bewindvoerders en ouders digitaal zaken kunnen doen voor hun klanten of voor hun kinderen.

3.2 Wettelijke verplichtingen

Besluit beveiligde verbindingen

Het besluit beveiligde verbindingen stelt het gebruik van beveiligingstandaarden (HTTPS, HSTS en maatregel 5 bij beveiligingsrichtlijn U/WA.05 van de Webapplicatie-richtlijn) verplicht voor alle publieke toegankelijke websites waarvan een bestuursorgaan de 'afzender' is. Dit betekent dat alle websites van provincies, waterschappen en hun samenwerkingsverbanden aan deze eisen moeten voldoen. Het Forum Standaardisatie rapporteert jaarlijkse in monitorstandaarden over toepassing van deze standaard. Er is ook een tool beschikbaar (internet.nl) waarmee gecontroleerd kan worden of een website voldoet.

Wat is nieuw voor bestuursorganen?

Bovengenoemde verplichtingen staan al langer op de 'pas toe en leg uit' lijst van Forum Standaardisatie en zijn ook in de commerciële sector breed en wijd geaccepteerd. Forum Standaardisatie doet elk half jaar een onderzoek naar de adoptie van deze standaarden. Daaruit blijkt dat 94% van alle bekende domeinnamen van bestuursorganen voldoet aan HTTPS en 85% aan HSTS. Er is ook een handige tool (internet.nl) om dat te toetsten. Deze tool is ook te gebruiken om periodiek in bulk websites te checken. In de praktijk komen er nog een tweetal problemen voor bij dit besluit:

- Vaak blijken de standaarden wel aanwezig maar niet geheel conform de richtlijnen geconfigureerd te zijn, waardoor nog geen optimale veiligheid wordt afgedwongen.
- Niet alle bestuursorganen hebben volledig grip op de websites waar zij 'afzender' van zijn. Er is niet altijd en compleet en actueel overzicht van websites van een bestuursorgaan.

NB: Bestuursorganen (en aangewezen organisaties) noemt de wet- en regelgeving ook wel (publieke) dienstverleners.

Bevindingen documentstudie:

Het besluit digitale verbindingen maakt ondubbelzinnig duidelijk aan welke eisen bestuursorganen moeten voldoen.

3.2.2 Besluit digitale overheid

Het besluit digitale overheid:

1. regelt de verwerking en verstrekking van persoonsgegevens door de routeervoorziening. Een voorziening waarmee bestuursorganen via één 'loket' van meerdere inlogmiddelen gebruik kunnen maken (artikel 5a en 9a, Bdo);
2. maakt het versleuteld verwerken van het BSN nummer mogelijk (artikel 5 en artikel 9, Bdo);
3. stelt regels ten aanzien van informatieveiligheid ((artikel 16-19, Bdo) waaraan bestuursorganen moeten voldoen voor het verlenen van toegang tot hun elektronische diensten. Bestuursorganen kunnen aantonen dat zij aan deze regels voldoen middels een ISO 27001 certificaat van een gekwalificeerd auditor (artikel 21).
4. stelt regels over het loggen van het gebruik van ICT voorzieningen voor elektronische dienstverlening, de periodieke controle van die logbestanden en de maximale bewaartermijn van deze logbestanden (5 jaar) (artikel 23, Bdo);
5. legt de ontstane praktijk van de DigiD assessments vast (artikel 24, Bdo).

Wat is nieuw voor bestuursorganen?

Routeervoorziening: De routeervoorziening is voor bestuursorganen nieuw en kan bestuursorganen ontzorgen bij het (verplicht) accepteren van de erkende inlogmiddelen. Een bestuursorgaan hoeft nog maar één verbinding te leggen om alle erkende inlogmiddelen te accepteren. Aansluiting op de routeervoorziening zal, volgens BZK, vergelijkbaar zijn met het aansluiten op DigiD. Op onderdelen zal het ongetwijfeld iets ingewikkelder zijn dan aansluiten op een enkelvoudig inlogmiddel als DigiD.

Versleuteld BSN: Het BSN nummer zal in de toekomst versleuteld verwerkt worden door de betrokken voorzieningen. Het versleutelen van het BSN waarborgt de privacy van burgers beter. En maakt het verstrekken van het BSN via private inlogmiddelen mogelijk. Inwoners kunnen dan gebruik maken van een privaat inlogmiddel zonder dat hun BSN buiten het overheidsdomein is in te zien. Bestuursorganen zullen zich moeten melden als BSN gerechtigde organisatie bij RvIG zodat zij het ontcijferde BSN via het identificatiestelsel kunnen ontvangen. Op termijn zullen bestuursorganen mogelijk zelf het BSN moeten ontcijferen, opdat de privacy van burger nog beter gewaarborgd wordt.

Informatieveiligheid: Op zichzelf zijn de informatieveiligheidsmaatregelen uit de Bdo niet nieuw. Deze maatregelen zijn opgenomen in de ISO27001 en zijn ook onderdeel van de BIO. En veel waterschappen en provincies zullen hier al in belangrijke mate aan voldoen of druk aan de slag om hier aan te gaan voldoen. De expliciete verwijzing naar certificering o.b.v. ISO 27001 is wel nieuw. De memorie van toelichting spreekt daarbij van een doelbepaling (m.a.w. het is wenselijk hier aan te voldoen). Dit is nieuw ten opzichte van de huidige situatie. Tot op heden is voor de waterschappen en de provincies de Baseline Informatieveiligheid Overheid (BIO) het leidende kader voor informatieveiligheid.

Logging: Het wettelijk verplicht loggen van gebruik van de ICT voorzieningen voor elektronische diensten is nieuw maar niet ongebruikelijk en sluit aan bij algemene 'best practices' en de AVG ter voorkoming van misbruik. Dit artikel legt daarmee de wettelijke basis om over het gebruik van de voorzieningen, persoonsgegevens in logbestanden te verzamelen. De precieze scope van logging is echter nog niet bepaald. Het besluit noemt naast enkele gedefinieerde gegevens zoals het gebruikte inlogmiddel en het BSN ook in algemene zin gegevens van systeemtechnische aard. Het is niet bekend wat onder gegevens van systeemtechnische aard wordt verstaan.

DigiD audits: Artikel 24 legt de over de afgelopen jaren ontstane praktijk rond DigiD audits wettelijk vast in plaats van in de aansluitvoorwaarden op DigiD van Logius. Er is dus voor bestuursorganen die al gebruik maken van DigiD weinig nieuws. Indien een bestuursorgaan nog geen aansluiting op DigiD heeft zal dit wel nieuw voor hen zijn.

Bevindingen documentstudie

- Artikel 21 van de Bdo maakt niet duidelijk wat nu van bestuursorganen wordt verwacht. Waterschappen en provincies werken al geruime tijd aan de implementatie van de BIO. Zowel de BIO als de ISO 27001 zijn breed geaccepteerde (en gerelateerde) normenkaders voor informatieveiligheid. Maar deze normenkaders zijn wel anders. Bij de ISO 27001 ligt de nadruk meer op het beheersproces en de mate waarin planmatig vanuit een risicoperspectief aan de implementatie van maatregelen wordt gewerkt. De BIO focust meer op de te nemen maatregelen om aan bepaalde beveiligingsniveaus te voldoen. Het is gedurende het onderzoek niet duidelijk wat de minister precies voor ogen heeft met dit artikel.

- De verwijzing naar gegevens van systeemtechnisch aard in artikel 23 die gelogd dienen te worden, maakt de voorziene scope van logging onbekend. De precieze scope van de logging is daarmee nog niet bepaald. En dat is bepalend voor de impact op bestuursorganen.
- De overige artikelen van het besluit digitale overheid zijn voldoende duidelijk en sluiten aan bij de huidige praktijk.

3.2.3 Regeling betrouwbaarheidsniveaus

De regeling schrijft voor hoe bestuursorganen de betrouwbaarheid van hun diensten moeten inschalen, gelet op de risico's. De dienstverlener bepaalt in beginsel ook het betrouwbaarheidsniveau van een machtiging. Voor de inschaling van de overheidsdienstverlening kiest deze regeling voor eenzelfde inschaling met de betrouwbaarheidsniveaus laag, substantieel en hoog, zoals in eIDAS. Het is aan bestuursorganen zelf om de risicoanalyse te maken aan de hand van het normatieve kader uit de regeling en noodzakelijke maatregelen te treffen. Daarvoor is een online regelhulp in de maak.

Wat is er nieuw voor bestuursorganen?

Classificeren van diensten is niet nieuw, ook nu al is het nodig vast te stellen op welk betrouwbaarheidsniveaus diensten worden aangeboden. In de Wdo is er voor gekozen om de vaststelling van de mate van toegangscontrole en de keuze voor het toegangsmiddel niet langer vrijblijvend te laten zijn, maar een verplichtend karakter te geven. Deze regeling heeft het karakter van een besluit van algemene strekking, zijnde een algemeen verbindend voorschrift. Het bestuur zal dan ook een besluit moeten en de strekking van dat besluit op moeten publiceren.

Bevindingen documentstudie

De regeling betrouwbaarheidsniveaus maakt voldoende duidelijk wat van bestuursorganen wordt verwacht. Ook zijn er voldoende hulpmiddelen beschikbaar om bestuursorganen daarbij te ondersteunen.

3.2.4 Regeling aansluitschema

Publieke dienstverleners dienen een datum op te geven waarop ze aangesloten zijn op de infrastructuur van het identificatiestelsel. Op de opgegeven data treedt de acceptatieplicht (artikel 7 en art 15 van de Wdo) in werking. Op dit moment gaat het om de volgende onderdelen van de infrastructuur:

- DigiD
- DigiD Machtigen
- erkende en toegelaten bedrijfs- en organisatiemiddel
- eIDAS-voorziening

De regeling benoemt ook de eNIK en het eRijbewijs als onderdelen van de infrastructuur, echter provincies en waterschappen spelen geen rol in de uitgifte van deze middelen.

Om aan te sluiten op het identificatiestelsel en daarmee te voldoen aan de acceptatieplicht van de Wdo, kunnen publieke dienstverleners verschillende wegen bewandelen:

1. Rechtstreeks aansluiten op de erkende en toegelaten middelen.
2. Aansluiten via de routeervoorziening van Logius (Identity Bridge).
3. Aansluiten via een commerciële intermediair.
4. Aansluiten als groep van waterschappen en/of provincies en een cluster aansluiting realiseren op de routeervoorziening.

De routeervoorziening is vanuit de minister de beoogde route om aan te sluiten. Het ontzorgt publieke dienstverleners en realiseert voor hen een enkelvoudig loket voor de aansluiting op het identificatiestelsel. Op dit moment ondersteunt de routeervoorziening alleen DigiD en eIDAS. eHerkenning en de andere componenten van het identificatiestelsel moeten nog ontsloten worden via de routeervoorziening.

De mogelijkheid van een cluster aansluiting is een nieuwe mogelijkheid. In de zorg is er inmiddels een pilot geweest voor de aansluiting van huisartsen op DigiD via een cluster aansluiting, maar de resultaten hiervan zijn onbekend. Het voordeel hiervan is dat er maar één keer een aansluittraject voor meerdere organisatie moet worden doorlopen. Tevens levert het, naar verwachting, een besparing op in de auditlasten voor de jaarlijkse benodigde audit. Het vereist echter wel dat de samenwerkende organisaties allen gebruik maken van dezelfde voorziening voor de toegang tot de digitale dienstverlening.

Bevindingen documentstudie

- De regeling aansluitschema maakt in beginsel voldoende duidelijk waaraan bestuursorganen moeten voldoen.
- Het is op dit moment niet bekend wanneer de overige componenten van het identificatiestelsel via de routeervoorziening ontsloten worden. Dit maakt het voor provincies en waterschappen dan ook lastig om op dit moment te bepalen wanneer zij op de routeervoorziening aan kunnen sluiten.
- Er is over de mogelijkheid van een cluster aansluiting op de routeervoorziening nog weinig informatie en ervaringen beschikbaar. Dit maakt het voor provincies en waterschappen op dit moment lastig te bepalen of dit een gunstige aansluitstrategie is en aan welke randvoorwaarden dan voldaan dient te worden.

3.2.5 Interbestuurlijk toezicht (art. 17, lid 3 Wdo)

De Wdo geeft in artikel 17 aan dat provincies toezicht op waterschappen en gemeenten dienen te houden op de naleving van artikelen art 3, 6, 7, 8 lid 1 en 15 van de Wdo. De Wdo verplicht daarbij de minister te informeren over de naleving van deze wet.

- Artikel 3: betreft de beveiligde verbindingen zoals uitgewerkt in besluit beveiligde verbindingen.
- Websites van gemeenten en waterschappen voldoen aan het bepaalde in besluit beveiligde verbindingen (https, hsts, het 'slotje' op de browser).
- Artikel 6: betreft de classificatieniveaus van diensten, zoals uitgewerkt in de regeling betrouwbaarheidsniveaus.
- Gemeenten en waterschappen hebben voor de diensten die zij digitaal aanbieden, bepaald welke gegevens worden uitgewisseld en het daarbij behorende betrouwbaarheidsniveau vastgesteld. Het bestuur van gemeenten en waterschappen hebben daartoe een besluit genomen en de strekking van dit besluit is gepubliceerd.
- Artikel 7 en 15: betreffen de acceptatieplicht van de erkende en toegelaten (publieke) inlogmiddelen zoals vastgelegd in besluit digitale overheid en de regeling aansluitschema
- Gemeenten en waterschappen accepteren alle dan toegelaten en erkende inlogmiddelen voor natuurlijke personen (art 7) en rechtspersonen (art 15) op het door het desbetreffende waterschap en gemeenten opgegeven moment van aansluiting.
- Art 8 lid 1: Een publiek middel en de (machting) voorziening worden uitsluitend gebruikt voor de toegang tot elektronische dienstverlening door bestuursorganen.
- Gemeenten en waterschappen gebruiken de erkende en toegelaten inlogmiddelen uitsluitend voor openbare, publiekrechtelijke taken.

Wat is nieuw voor bestuursorganen?

De Wdo geeft provincies een specifieke toezichtstaak op een nieuw terrein namelijk de digitale overheid. Dat is nieuw voor provincies want zij hebben op dit vlak op dit moment geen taak en dus ook geen expertise (anders dan voor hun eigen bedrijfsvoering). Voor waterschappen en gemeenten betekent het dat zij een informatieverplichting over de naleving van de Wdo richting provincies krijgen. Immers, de provincies moeten de minister kunnen informeren over de naleving van de Wdo.

Bevindingen documentstudie

- De wet en toelichting geven geen duidelijkheid of het bij de toezichtsrol van Gedeputeerde Staten om medebewind gaat of niet. Daarnaast is onduidelijk of de aan Gedeputeerde Staten opgelegde toezichtstaak in lijn is met bestaande wetgeving (Gemeentewet, Provinciewet, Financiële verhoudingswet, Wet revitalisering generiek toezicht).
- In een eerder stadium heeft de Afdeling advisering van de Raad van State al geadviseerd nader te kijken naar de toezichtsbepalingen in de Wdo⁷: “Het generieke toezicht is bedoeld als sober en terughoudend en in hoofdzaak gericht op bestuurlijke en financiële verhoudingen. Het is bedoeld noch ingericht voor technische, organisatorische en uitvoerende kwesties, zoals die zich voordoen in de digitale (overheids-)infrastructuur. De vormgeving van het bestuurlijk toezicht moet om die reden opnieuw worden doordacht en het voorstel moet vervolgens worden aangepast”. Dit heeft toen niet geleid tot aanpassingen van het wetsvoorstel.
- Uitgangspunt van de Wet revitalisering generiek toezicht is dat gemeenten en waterschappen met één toezichthouder per beleidsterrein te maken hebben. Straks houden de provincies toezicht op onderdelen van de Wdo die op zijn minst bijvoorbeeld het toezicht raken van de minister van BZK op het gebruik van DigiD of het toezicht van de inspectie SZW op bijvoorbeeld informatieveiligheid in het sociaal domein.
- De Wdo reikt provincies geen andere instrumenten aan dan de bestaande mogelijkheid van schorsing, indeplaatsstelling en het doorlopen van de interventieladder. De vraag is, gegeven de dynamiek in de digitale overheid, of dit instrumentarium in de praktijk toereikend is. Als bijvoorbeeld bepaalde (gevoelige) elektronische diensten op een te laag betrouwbaarheidsniveau worden aangeboden, dan kan gedeputeerde staten niets anders dan bovengenoemde instrumenten inzetten, terwijl er mogelijk ook effectievere en meer passende instrumenten mogelijk zijn. De minister krijgt voor zijn nieuwe toezichtstaak naast de generieke instrumenten ook zeer specifieke instrumenten waarmee technisch ingegrepen kan worden en snel een eind aan een overtreding gemaakt kan worden. Dat geeft een indicatie van de benodigde slagkracht op dit dynamische taakgebied, die Gedeputeerde Staten ontberen.
- De dynamiek van het huidige stelsel heeft in de twaalf (onderling) verschillende provincies (Noord-Brabant telt 61 gemeenten, Limburg 31, Flevoland 6) tot een generiek toezicht op maat geleid. De manier waarop het toezicht in de Wdo is neergelegd doorkruist dat.
- Het is op dit moment niet bekend welke informatie, op welk detail- of kwaliteitsniveau, op welk moment en met welke frequentie de minister over de naleving van de Wdo van Gedeputeerde Staten wenst te ontvangen. De informatieplicht in de Wdo lijkt verder niet te stroken met de Wet revitalisering generiek toezicht, waarbij Gedeputeerde Staten beleidsvrijheid hebben ten aanzien van het uitvoeren van hun toezicht.
- De capaciteitsvraag en benodigde expertise en financiën zijn nog onbekend. Vermoedelijk zullen Gedeputeerde Staten de toezichtstaak niet kunnen neerleggen bij de expertise die zij al in huis hebben. Immers deze is ingezet voor de eigen bedrijfsvoering. Bovendien zullen mogelijke interventies veel meer capaciteit gaan vergen dan nu gebruikelijk is bij het interbestuurlijk toezicht. Verder is onduidelijk welke middelen de provincies krijgen om de nieuwe taken uit te voeren.

⁷ Tweede Kamer, vergaderjaar 2017–2018, 34-972, nr. 4, pagina 4:

3.3 Samenhang met andere wetgeving

De Wdo staat niet op zichzelf. Er zijn meerdere wetten die iets zeggen over digitale dienstverlening van bestuursorganen.

De Wdo regelt (in deze tranche) vooral de wijze waarop elektronische dienstverlening tot stand komt en hoe de toegang daartoe is geregeld. Direct aanpalend aan de Wdo zijn er aantal wetten die ook toezien op de elektronische dienstverlening van bestuursorganen.

- De wet modernisering bestuurlijk elektronisch verkeer (Wmbev) geeft de burger recht op het elektronisch zakendoen met bestuursorganen. Verwachte in werking treding is 1 juli 2022.
- In de Single Digital Gateway verordening is bepaald dat een aantal diensten volledig digitaal Europees beschikbaar en vindbaar moeten zijn. Inwerkingtreding is voorzien eind 2023.

Deze twee wetten verplichten bestuursorganen dan ook diensten digitaal aan te gaan bieden. De Wdo bepaalt vervolgens hoe de toegang tot die diensten geregeld dient te zijn. Daarnaast is er het tijdelijk besluit digitale toegankelijkheid die vervolgens eisen stelt aan de inhoudelijke vormgeving van deze digitale diensten, zodat ook mensen met een beperking ervan kunnen gebruikmaken.

De Algemene verordening gegevensbescherming (AVG) en de Baseline Informatieveiligheid Overheid (BIO) zijn in dit verband ook relevant. De Wdo sluit bij deze bestaande wet en regelgeving aan. Zo bepalen de AVG en BIO nu al dat gegevens geclassificeerd moeten zijn en dat bepaalde minimale eisen ten behoeve van gegevensbescherming genomen moeten worden. De Wdo bouwt hier op door.

HOOFDSTUK 4

Impact op provincies en waterschappen

In dit hoofdstuk gaan we nader in op de impact van de invoering van de Wdo op provincies, waterschappen, belastingkantoren en omgevingsdiensten. Deze impact is in kaart gebracht door analyse van de survey resultaten, de gevoerde gesprekken en de workshops. We gaan achtereenvolgens in op de volgende hoofdonderwerpen:

- Dienstverlening
- Informatiebeveiliging en ICT
- Bestuur en organisatie
- Financieel

Deze hoofdonderwerpen zijn uitgesplitst naar verschillende deelonderwerpen. De paragrafen zijn als volgt opgezet: we beginnen met een analyse van de survey resultaten en deze vullen we aan met input vanuit de workshops. We geven per vraag met N aan door hoeveel respondenten de vraag is beantwoord. We tonen per onderwerp steeds één grafiek met survey resultaten ter illustratie. De overige grafieken (met resultaten van alle vragen uit de survey) zijn in de separate bijlage gepresenteerd. Elk hoofdonderwerp eindigen we met een tussenconclusie. De overall conclusies en aanbevelingen worden gepresenteerd in hoofdstuk 5.

4.1 Impact dienstverlening

4.1.1 Inlogmiddelen

Om de voortgang van digitale dienstverlening te kunnen waarborgen worden meer inlogmiddelen toegelaten. Daarvoor geldt dan een acceptatieplicht, te weten voor toegelaten identificatiemiddelen, erkende middelen en bij de Europese Commissie genotificeerde middelen. Het gebruik van andere inlogmiddelen, zoals de eigen inlogmiddelen van organisaties, zal in de meeste gevallen niet meer zijn toegestaan.

Analyse survey resultaten

- **Aansluiting op DigiD (N=41).** De meeste organisaties zijn reeds aangesloten op DigiD (75%, N=41). Een enkeling (m.n. omgevingsdiensten) nog niet.
- **Aansluiting eHerkenning.** De meeste organisaties (78%, N=41) zijn aangesloten op eHerkenning en een aantal (7%, N=41) werken er aan.
- **Aansluiting BSN koppelregister en DigiD Machtigen.** Bijna geen enkele organisatie is aangesloten op het BSN koppelregister (83%, N=40) en DigiD Machtigen, (85%, N=40) op een paar organisaties na.
- **Aansluiting eIDAS.** Voor eIDAS (N=39) zien we de grootste spreiding, 36% van de organisaties is wel aangesloten, 44% niet en 15% werkt eraan. Ongeveer de helft van de waterschappen, provincies en belastingkantoren is aangesloten, de meeste omgevingsdiensten nog niet.

- **Acceptatieplicht.** We hebben de respondenten gevraagd welke gevolgen de acceptatieplicht voor hen heeft. De meest genoemde antwoorden zijn:
 - technische inrichting, processen;
 - beheer en governance moeten worden ingericht;
 - het moet mogelijk worden om met een machtiging in te loggen;
 - registratie van aanvragen inrichten in zaaksysteem;
 - treffen van extra maatregelen om voldoende mate van beveiliging te kunnen bieden;
 - e-formulieren aanpassen;
 - capaciteit en budget vrijmaken en het informeren van de organisatie.

Afhankelijkheid van contracten en planning van leveranciers speelt bij een flink aantal organisaties een rol. Bij inschatting van de grootte van deze gevolgen (N=41) geeft 12% aan dat deze groot zijn, 45% gemiddeld, 32% klein en 11% weet het niet. Bij de belastingkantoren en waterschappen is de grootste spreiding te zien. Van alle waterschappen geven relatief gezien de meeste organisaties aan dat de gevolgen groot zijn (23,53%), terwijl de meeste organisaties van de omgevingsdiensten aangeven dat de gevolgen klein zijn (70%).

“Het accepteren van meer authenticatiemethodieken heeft stevige impact op de organisatie, mede omdat extra maatregelen noodzakelijk zijn om een voldoende mate van beveiliging van dienstverlening te kunnen blijven realiseren (hoe meer deuren je in je huis plaats, hoe meer sloten je dient plaatsen)”

| Quote van een waterschap |

- De meeste organisaties (40%, N=40) verwachten een gemiddelde inspanning te moeten verrichten om te voldoen aan de acceptatieplicht. Maar er is veel spreiding te zien, dus de opvattingen lopen behoorlijk uiteen (zie figuur 4). Qua inspanning (N=40) verwachten de meeste organisaties (53%) dat het voldoen aan de acceptatieplicht veelal structureel zal zijn. Tegelijkertijd schat een flink aantal respondenten (30%) dat de inspanningen tijdelijk zijn.

Niet ingevuld



(4) Groot



(3) Gemiddeld



(2) Klein



(1) Zeer klein



■ Provincies ■ Waterschappen
■ Belastingkantoren ■ Omgevingsdiensten

Figuur 4. Antwoorden op de vraag: 'Hoe groot schat u de inspanning om aan de acceptatieplicht te voldoen?'

Input workshops

Voor wat betreft aansluiting op het BSN koppelregister, DigiD Machtigen en eIDAS geven respondenten aan dat de aansluiting veelal nog niet geregeld is, omdat de behoefte/gebruik laag is, er nog geen wettelijke verplichting was, er gebrek aan capaciteit is, men onbekend is met de regeling en omdat er geen testmiddelen (voor eIDAS) zijn. Ook moeten nut opwegen tegen kosten. V.w.b. de acceptatieplicht blijkt dat veel organisaties nog kennis moeten opdoen om dit goed te regelen. Ook geven respondenten aan dat de impact op de organisatie lastig te bepalen is, omdat er nog inventarisaties van het werk moeten plaatsvinden. Aangegeven wordt dat de structurele inspanning vooral zit in het monitoren van toelatingen van inlogmiddelen, het (functioneel) beheer, controle op processen, kennis up-to-date houden, audits en de governance. Aangegeven wordt dat de tijdelijke inspanning vooral zit in de aansluiting, realiseren van koppelingen, testen, inrichten van processen en het op orde brengen van de techniek.

4.1.2 Routeervoorziening

Om de publieke dienstverleners te ontzorgen, kunnen zij via één ontsluitende dienst (routeringsvoorziening die de toegang tot elektronische dienstverlening faciliteert) worden aangesloten op de toegelaten en erkende inlogmiddelen. Het inloggen verloopt in dat geval via één aansluiting, ongeacht welk inlogmiddel gebruikt wordt. Dit is niet verplicht. Dienstverleners kunnen er tevens voor kiezen zelf aansluitingen te organiseren met losse koppelingen of dit uit te besteden aan een private partij.

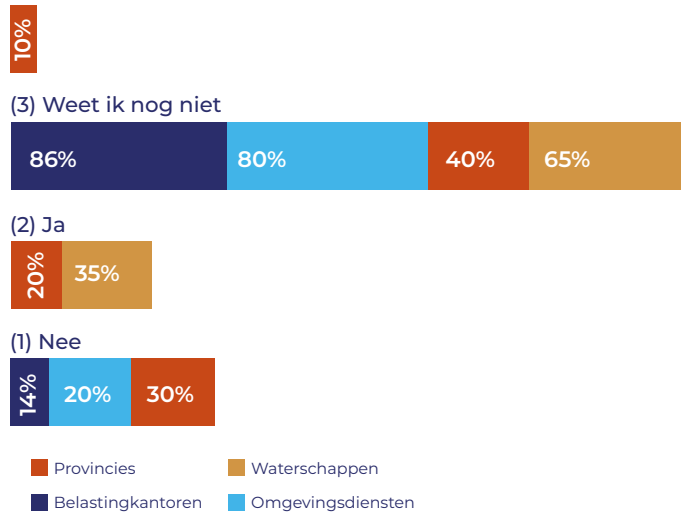
Er zijn vier routes om te voldoen aan de acceptatieplicht:

1. Rechtstreeks aansluiten op erkende en toegelaten middelen.
2. Aansluiten via de routeervoorziening van Logius.
3. Aansluiten via een commerciële intermediair.
4. Aansluiten als groep van waterschappen of provincies en een cluster aansluiting nemen op de routeervoorziening.

Analyse survey resultaten

- Voor wat betreft aansluiting op de routeervoorziening (N=38) zegt het overgrote merendeel (64%) van de respondenten nog niet te weten of ze willen aansluiten op de routeervoorziening (zie figuur 5). Een kleine groep (15%) zegt nee en een kleine groep (21%) gaat dit wel doen. Bij provincies is de grootste spreiding in antwoorden te zien. De helft van de waterschappen weet nog niet of ze gaan aansluiten en de andere helft geeft aan dit wel te willen doen. Geen enkel belastingkantoor of omgevingsdienst wil nu aansluiten.
 - Van de respondenten die aangeven wel aan te willen sluiten op de routeervoorziening (N=13), geeft 31% aan dat dit geen tot beperkte impact heeft op de organisatie, 54% zegt gemiddelde impact en 15% grote impact. Tevens geeft 57% (N=14) aan dat de inspanningen om aan te sluiten veelal structureel zullen zijn, tegenover 29% (N=14) van de respondenten die dit voornamelijk als tijdelijk inschat. De meningen over de duur van de inspanningen zijn bij provincies en waterschappen verdeeld. Het merendeel van de provincies denkt aan een tijdelijke inspanning, terwijl het merendeel van de waterschappen aan een structurele inspanning denkt. De grootte van de inspanning (N=13) wordt door 8% als zeer klein ingeschat, door 62% als gemiddeld en door 30% als groot.
 - Van de organisaties die aangeven niet aan te willen sluiten op de routeervoorziening (N=11) zegt 64% dat dit beperkte impact op de organisatie heeft, 9% gemiddelde impact en 27% grote impact. De inspanning hiervan (N=11) wordt door 55% als tijdelijk ingeschat, door 27% als structureel en 18% weet het niet. De inspanning om de koppelingen zelf te organiseren (N=10) wordt door 50% van de respondenten als zeer klein tot klein ingeschat, door 10% als gemiddeld en 40% als groot tot zeer groot.

Niet ingevuld



Figuur 5. Antwoorden op de vraag: 'Gaat uw organisatie naar verwachting gebruik maken van de routeervoorziening?'

- Volgens de respondenten is de routeervoorziening van toegevoegde waarde als deze op een laagdrempelige manier geïmplementeerd kan worden, als er minder te onderhouden koppelingen zijn, als deze goedkoper, bewezen betrouwbaar, eenvoudig aan te sluiten en toekomstvast is, er geen DigiD-audit nodig is, het volledig ontzorgt, het minder werk is dan de individuele koppelingen, weinig onderhoud vergt en wanneer dit de klantreis van klanten verbetert/vereenvoudigt. Wel wordt aangegeven dat er eerst meer koppelingen ontsloten moeten worden, voordat het interessant wordt.
- Acties voor aansluiting betreffen: bestaande eDienstverleningsportal aanpassen, aangesloten applicaties opnieuw koppelen, bestaande aansluitingen omzetten vanuit Enterprise Service Bus naar de routeringsvoorziening van Logius, impactanalyses uitvoeren en een visie opstellen.
- Organisaties die niet willen aansluiten op de routeervoorziening geven als reden: 'Wij maken gebruik van een derde partij die ons ontzorgt betreffende de aansluiting op generieke landelijke voorzieningen zoals DigiD, eIDAS, e-herkenning, basisregistraties en DSO'; 'We gebruiken alleen DigiD via een e-loket'; 'Ten eerste, deze voorziening is te laat gereed, ten tweede, de belangrijkste voorziening voor de provincie is eHerkenning, en die wordt juist niet aangeboden door Logius, ten derde, de provincie heeft reeds meer dan een jaar de voorziening operationeel voor eHerkenning, eIDAS en DIGID o.b.v. private leverancier'; 'Onvoldoende inzicht in voordelen t.o.v. huidige situatie'.

- Als bestuursorganen zelf de aansluiting gaan regelen, vergt dit de volgende acties: 'Regelen van de juiste machtigingen om de derde partij namens ons de koppelingen te laten realiseren'; 'Bij nieuwe applicaties dienen we deze opnieuw te koppelen'; 'Leverancier van de e-formuliergevoorziening zal de koppelingen moeten realiseren'.

Input workshops

Veel respondenten geven aan voorkeur voor de routeervoorziening van Logius te hebben, maar hebben behoefte aan meer informatie, onder meer over: kosten/baten, randvoorwaarden en voor- en nadelen. Daarnaast moeten eerst alle koppelingen ontsloten worden, anders is de toegevoegde waarde te beperkt voor de bestuursorganen.

4.1.3 Betrouwbaarheidsniveaus

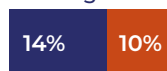
De wet regelt dat inloggen bij publieke diensten waarbij gegevensuitwisseling plaatsvindt, op een adequaat betrouwbaarheidsniveau moet gaan plaatsvinden. Alle dienstverleners met een publieke taak moeten voor de diensten die zij verlenen zelf het betrouwbaarheidsniveau bepalen (laag, substantieel, hoog) aan de hand van het gestelde normenkader in de Regeling betrouwbaarheidsniveaus.

Analyse survey resultaten

- De Commissie Bestuurszaken, Communicatie en Financiën (CBCF) heeft voor de waterschappen een inschaling van betrouwbaarheidsniveaus voor digitale diensten vastgesteld, op voorspraak van de themagroep dienstverlening. Het Forum Standaardisatie heeft een handreiking (regelhulp) voor alle bestuursorganen opgesteld voor de betrouwbaarheidsniveaus.
 - Inschaling CBCF. Van de waterschappen (N=11) heeft 1 waterschap helemaal geen gebruik gemaakt van deze inschaling, 9 gedeeltelijk en 1 volledig.
 - Handreiking Forum Standaardisatie. Van de provincies (N=8) hebben 2 organisaties de handreiking helemaal niet gebruikt, 4 gedeeltelijk en 2 volledig. Van de waterschappen (N=15) hebben 4 organisaties de handreiking helemaal niet gebruikt, 10 gedeeltelijk en 1 volledig.
- Op dit moment heeft 15% van de organisaties (N=41) al een volledige inschaling van de betrouwbaarheidsniveaus van digitale dienstverlening gemaakt, tegenover 29% die dat nog helemaal niet heeft gedaan en 56% die dit gedeeltelijk heeft gedaan (zie figuur 6). Van de respondenten (N=40) denkt 63% dat de inspanningen om de inschaling te kunnen maken structureel zijn en 28% denkt tijdelijk. De overige respondenten weten het niet.

De inspanningen om te kunnen voldoen (N=38) worden door 53% van de respondenten als gemiddeld ingeschat, 29% schat groot en 18% denkt zeer klein tot klein.

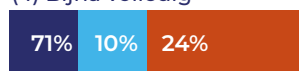
Niet ingevuld



(5) Volledig



(4) Bijna volledig



(3) Gemiddeld



(2) In enige mate



(1) Helemaal niet



Provincies Waterschappen
Belastingkantoren Omgevingsdiensten

Figuur 6. Antwoorden op de vraag: 'In hoeverre heeft er al een inschaling van betrouwbaarheidsniveaus van digitale dienstverlening plaatsgevonden in uw organisatie?'

Om te voldoen aan de Regeling Betrouwbaarheidsniveaus moet een herijking van benodigde betrouwbaarheidsniveaus bij digitale diensten plaatsvinden; diensten moeten geclassificeerd worden bij bestuursbesluit en formeel bekendgemaakt. Op basis daarvan moeten eventueel maatregelen worden genomen; contracten met leveranciers moeten gecontroleerd worden of deze voldoen aan de wet, de genomen besluiten en afspraken; regelingen moeten gelezen worden en er moet worden gecheckt wat er wordt gevraagd; er moet gewerkt worden aan inventarisatie, het informeren van collega's, implementeren, het opnemen in de SLA en beheer.

Input workshops

De aanwezigen in de workshops onderschrijven het beeld dat ontstaat uit de survey. Daarnaast is gevraagd naar de betrokkenheid van het bestuur op dit onderwerp. Een aantal organisaties heeft de betrouwbaarheidsniveaus laten vaststellen door het bestuur, maar een flink aantal ook niet.

4.2 Tussenconclusies dienstverlening

Inlogmiddelen. Op dit moment zijn de meeste bestuursorganen aangesloten op DigiD en eHerkenning. Aansluiting op eIDAS, DigiD Machtigen en het BSN koppelregister is veelal nog niet geregeld, omdat behoefte/gebruik laag is, er nog geen wettelijke verplichting was en er sprake is van veel onbekendheid. Uit de survey blijkt dat de acceptatieplicht voor een kwart van de respondenten van de waterschappen grote gevolgen heeft, terwijl de andere bestuursorganen vaker gemiddeld aangeven. Bijna driekwart van de omgevingsdiensten geeft zelfs aan dat de gevolgen klein zijn. Om te kunnen voldoen aan de verplichting tot acceptatie van alle erkende inlogmiddelen, moeten zowel tijdelijke als structurele inspanningen geleverd worden. Uit de survey en workshop blijkt dat er nog veel sprake is van onbekendheid op dit vlak, daardoor vinden betrokkenen het lastig om de precieze impact op de organisatie te kunnen bepalen.

Routeervoorziening. Door onduidelijkheid, onbekendheid en informatiegebrek weten verreweg de meeste bestuursorganen nog niet of ze op de routeervoorziening van Logius willen aansluiten. Als we inzoomen op de verschillen tussen de bestuursorganen blijkt uit de survey dat de waterschappen wat positiever tegenover aansluiting staan: deze geven aan het nog niet te weten of wel te willen aansluiten. Geen enkel belastingkantoor of omgevingsdienst geeft aan te willen aansluiten. De meerwaarde van de routeervoorziening wordt ingezien als op een laagdrempelige manier aangesloten kan worden, als de voorziening betrouwbaar is, écht ontzorgt en de kosten en baten tegen elkaar opwegen. Een aantal bestuursorganen wil niet aansluiten omdat de voorziening te laat (i.e. volledig met alle koppelingen) gereed is en onduidelijk is wat de voordelen, kosten en baten precies zijn.

Betrouwbaarheidsniveaus. Om te voldoen aan de Regeling Betrouwbaarheidsniveaus moet een herijking van benodigde betrouwbaarheidsniveaus bij digitale diensten plaatsvinden. De te leveren inspanningen zijn voor bestuursorganen duidelijk, maar beslaan wel veel werk.

4.3 Impact informatieveiligheid en ICT

4.3.1 Beveiligde verbindingen

Het besluit beveiligde verbindingen verplicht het gebruik voor van een aantal standaarden voor beveiligde verbindingen, te weten HTTPS, HSTS en TLS 1.2 en maatregel 5 van de UA/W01 van de webapplicatierichtlijnen. Deze verplichting geldt voor alle publiek toegankelijke websites waarvoor bestuursorganen verantwoordelijk zijn.

Analyse survey resultaten

- De meeste respondenten (93%, N=44) hebben voldoende tot volledig overzicht over de websites waar zij verantwoordelijk voor zijn (zie figuur 7). Van deze websites voldoet ca. 77% aan de genoemde standaarden. De acties die ondernomen moeten worden om te voldoen zijn: inventarisatie van websites, monitoring, verantwoordelijkheden beleggen, governance inregelen, het uitvoeren van een maandelijkse 'vulnerability scan', beleid maken en implementeren, leveranciersmanagement verbeteren, aanpassen van SLA's en het aanspreken van andere website-eigenaren waaronder gemeenschappelijke regelingen en publiek-private samenwerkingen.
- De inspanning om zorg te dragen dat al deze websites voldoen aan de veiligheidsstandaarden (HTTPS en HSTS) is (N=44) bij de meeste respondenten (54%) klein tot zeer klein, 34% gemiddeld en 12% groot tot zeer groot. Deze inspanningen (N=44) worden door de meeste respondenten als structureel (59%) ingeschat en door 34% als tijdelijk. De overige organisaties weten dit nog niet.

(5) Volledig overzicht



(4) Veel overzicht



(3) Voldoende overzicht



(2) Beperkt overzicht



(1) Geen overzicht



Figuur 7. Antwoord op de vraag: 'In hoeverre heeft u het overzicht op alle publiek toegankelijke websites waar uw organisatie verantwoordelijk voor is?'

Input workshops

Er lijken weinig belemmeringen te zijn om te voldoen aan de gestelde eisen rondom de beveiligde verbindingen. De enige uitdaging is om alle websites, inclusief subdomeinen, up-to-date te houden.

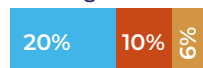
4.3.2 Logging

De wet bepaalt dat publieke dienstverleners logbestanden bijhouden over het gebruik van ICT voorzieningen voor toegang tot elektronische dienstverlening en deze regelmatig beoordelen. Het betreft uitgevoerde authenticaties, de daarbij gebruikte identificatiemiddelen, de tijdstippen waarop is ingelogd en uitgelogd, de systeemtechnische gegevens, waaronder het IP-adres en, indien van toepassing, machtigingsgegevens. Deze gegevens worden maximaal 5 jaar bewaard.

Analyse survey resultaten

- De respondenten (N=40) geven grote spreiding in hun antwoorden als gevraagd wordt naar de initiële inspanning om de logbestanden aan te maken (zie figuur 8), van zeer klein (8%), klein (32%), gemiddeld (22%), groot (33%) tot zeer groot (5%). Structureel verwachten (N=36) de meeste respondenten (57%) enkele dagen per maand nodig te hebben om de logbestanden goed te beheren, daarnaast denkt 26% dat het een redelijk omvangrijke taak betreft, 6% denkt één fte, 9% denkt meerdere fte's en 2% denkt geen extra inspanning.

Niet ingevuld



(5) Zeer groot



(4) Groot



(3) Gemiddeld



(2) Klein



(1) Zeer klein



Provincies Waterschappen
Belastingkantoren Omgevingsdiensten

Figuur 8. Antwoorden op de vraag: 'Hoeveel inspanning moet uw organisatie initieel leveren om de genoemde logbestanden aan te maken?'

- De acties die volgens de respondenten ondernomen moeten worden om de bedoelde logbestanden aan te kunnen maken zijn: 'Afspraken maken met de derde partijen in de SLA's, omdat die onderdeel is van de uitbestede diensten'; 'Geen, want de logbestanden worden bij de provider (webhost) bewaard'; 'De systemen verzamelen de benodigde logging informatie en de bronnen zijn er, maar er moeten nog acties worden uitgevoerd v.w.b. het centraal opslaan, doorzoekbaar maken en bewaren'; 'Inregelen bewaarplicht, monitoring, analyse'; 'Het ontvangen van bestanden m.b.t. het gebruik van identificatiemiddelen voor elektronische dienstverlening, qua vorm en frequentie moet dit worden georganiseerd met betrokken partijen'; 'De loggingsvoorziening moet worden gerealiseerd'; 'Beheerprocedures opstellen, opslag (archief) regelen, procedure voor gebruik opstellen, governance opstellen, prioritering op basis van classificatie'; 'Leveranciers moeten technische aanpassingen aanbrengen, daarnaast moeten beleid en controle mechanismen worden georganiseerd'; 'Inrichten logsystemen en aansluiten authenticatiesystemen'.

Input workshops

- Logging vergt veelal een grote inspanning. Er moet opslag en beheer worden geregeld (met goede vindbaarheid en doorzoekbaarheid) en dit moet weer beveiligd worden. Het proces moet worden ingericht en er moet worden bepaald wie wat mag opvragen onder welke voorwaarden. De permanente registratie heeft een structurele impact op de organisatie. Als alles uitbesteed wordt aan een externe leverancier is de inspanning voor bestuursorganen een stuk minder groot.
- Het is niet helemaal duidelijk wat de wetgever precies bedoelt met 'systeemtechnische gegevens'. Dit is in de wetstekst en memorie van toelichting onvoldoende gespecificeerd.

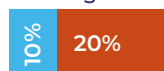
4.3.3 Informatiebeveiliging

Artikel 21 van het Besluit digitale overheid bepaalt dat bestuursorganen geacht worden te voldoen aan de gestelde eisen over informatieveiligheid (artikelen 16 tot en met 19). Deze artikelen zijn nieuw en brengen diverse verplichtingen met zich mee met betrekking tot informatieveiligheidsbeleid, organisatie en beheer, personele en fysieke beveiliging en ICT-voorzieningen en informatiesystemen. Artikel 21 bepaalt tevens dat bestuursorganen en aangewezen organisaties geacht worden aan de artikelen 16 tot en met 19 te voldoen indien zij aantoonbaar ISO/NEN 27001 en 27002 toepassen voor de toegang tot elektronische dienstverlening (en dus niet voor de hele organisatie).

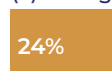
Analyse survey resultaten

- Informatiebeveiliging is bij veel respondenten (N=42) 'work in progress' (50%), 29% van de respondenten geeft aan dat hun organisatie nu al voldoet aan BIO of de ISO/NEN 27001 voor de toegang tot elektronische dienstverlening, tegen 10% die nog niet voldoet. De overige respondenten hebben 'anders' geantwoord.
- Het merendeel van de respondenten (51%, N=41) geeft aan dat de eisen van de ISO27001 en de BIO grote tot zeer grote impact op de organisatie hebben (zie figuur 9). De meeste organisaties (75%, N=41) hebben een plan om te voldoen aan de eisen m.b.t. informatiebeveiliging. De inspanning is volgens praktisch alle respondenten (95%, N=40) van structurele aard en neemt meer dan 4 maanden in beslag (79%, N=39). De inspanningen om te voldoen aan de maatregelen (N=40) wordt door 8% van de respondenten als zeer klein tot klein ingeschat, door 40% als gemiddeld, door 37% als groot en 15% als zeer groot.

Niet ingevuld



(5) Zeer grote impact



(4) Grote impact



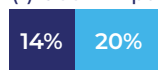
(3) Gemiddeld impact



(2) Beperkte impact



(1) Geen impact



Provincies Waterschappen
Belastingkantoren Omgevingsdiensten

Figuur 9. Antwoorden op de vraag: 'Welke impact hebben de eisen van de BIO of de ISO/NEN 27001 m.b.t. informatieveiligheid op uw organisatie?'

- De respondenten geven aan dat de volgende acties vereist zijn om te voldoen: 'Aan de hand van risico inventarisaties moeten er analyses worden gedaan van de BIO en ISO normen, die analyses leveren overzichten op van de punten waaraan moet worden voldaan en acties die nog moeten worden ondernomen'; 'Interne audit van alle genoemde maatregelen, certificeringsaudit uitvoeren door externe auditor'; 'Opname in PDCA cyclus; inrichten ISMS voor PDCA; specifiek toeschrijven van beleid gericht op toegang tot de elektronische dienstverlening en daarmee ook het eigenaarschap beleggen en de maatregelen die dat moeten borgen'; 'Processen (her)inrichten'; 'Medewerkers moeten hun werkwijzen aanpassen, opgeleid en bewust gemaakt worden'; 'Er moet input geleverd worden voor jaarlijkse audits (aantoonbaarheid inregelen)'; 'Er moet gewerkt worden aan detectie (inregelen specifieke logging en monitoring)'.

"Veel diverse acties welke betrekking hebben op zowel mens, organisatie als ook techniek"

| Quote |

Input workshops

In de workshops is de respondenten gevraagd naar het moment waarop ze verwachten te voldoen aan alle gestelde eisen vanuit de ISO/BIO. De meeste respondenten verwachten dat ze mogelijk certificeerbaar zijn voor ISO27001 op 1 juli 2022. Dit betekent niet dat ze ook daadwerkelijk gecertificeerd zullen zijn of worden.

4.4 Tussenconclusies Informatiebeveiliging en ICT

Beveiligde verbindingen. Er lijken weinig belemmeringen te zijn om te voldoen aan de gestelde eisen uit het besluit beveiligde verbindingen. Een belangrijke uitdaging is om het overzicht te houden over alle websites (zowel hoofd- als subdomeinen) en zorg te dragen dat deze up-to-date zijn en op de juiste wijze geconfigureerd. De meeste organisaties hebben goed zicht op de websites die zij in eigen beheer hebben.

Logging. De impact op bestuursorganen om te kunnen voldoen aan de eisen omtrent logging is groot. Beheer, opslag en het inrichten van processen vergen het meeste werk. Ook zijn de eisen aan wat er precies gelogd moet worden niet volledig duidelijk. Voornamelijk de 'systeemtechnische gegevens' zijn multi-interpretabel.

Informatiebeveiliging. De eisen aan informatieveiligheid zijn tamelijk groot, maar dit onderwerp staat bij de meeste bestuursorganen wel al goed op het netvlies. Overheidsorganisaties moeten zich conformeren aan de BIO, maar de Wdo verwijst naar de ISO. De eisen die de BIO stelt zijn niet één-op-één hetzelfde als de gestelde eisen vanuit de ISO.

4.5 Impact bestuur en organisatie

Het bestuur van organisaties staat voor de taak een aantal besluiten te nemen, teneinde de implementatie en naleving van de nieuwe wet- en regelgeving te borgen:

- Het classificeren van de diensten naar betrouwbaarheidsniveau zijn besluiten van algemene strekking, zijnde een algemeen verbindend voorschrift. Het vaststellen van de betrouwbaarheidsniveau vergt dan ook een besluit van het bevoegde gezag.
- Het bestuur zal ruimte moeten geven aan de realisatie en het beheer van de verplichtingen vanuit de Wdo.
- Het doorvoeren van de randvoorwaarden en verplichtingen die de wet stelt aan de processen van de organisatie. Diverse processen moeten worden aangepast en organisatorisch worden ingebed.

Het systeem als geheel verandert met de nieuwe wet- en regelgeving niet; het geheel van verantwoordelijkheden blijft onveranderd. Binnen het systeem ontstaan voor betrokkenen wel een aantal nieuwe verplichtingen, zoals eerder beschreven. De besluiten van de Wdo zullen dan ook geen grotere veranderingen in de organisatie teweeg brengen, maar dat laat onverlet dat die veranderingen in goede banen moeten worden geleid. Dat vraagt om heldere verantwoordelijkheden. Onze ervaring en de observatie van de begeleidingsgroep is echter dat de bestuurlijke verantwoordelijkheid voor wetgeving op digitaal gebied in de praktijk vaak onvoldoende geborgd is in een organisatie.

Interbestuurlijk toezicht

Er is vanuit provincies grote twijfel over de uitvoerbaarheid van het specifieke toezicht dat in de Wdo is opgenomen. Hoewel er nog veel onduidelijk is, verhoudt hetgeen nu in de Wdo staat, zich niet goed tot de wijze waarop provincies hun generieke toezicht hebben vormgegeven en tot hetgeen is bepaald in de Wet revitalisering generiek toezicht.

Het is daarbij op dit moment nog niet bekend welke informatie het ministerie van BZK wil ontvangen van provincies over de naleving van de Wdo. Dat maakt het lastig in te schatten wat dit precies van de provincies vereist.

Op dit moment hebben provincies op het gebied van de digitale overheid geen interbestuurlijke toezichtstaak, maar zij krijgen deze taak straks wel. Dat betekent dat zij daar de personele capaciteit, expertise en werkprocessen voor moeten gaan inregelen, om die taak te kunnen invullen. Organisatorisch en op personeel vlak heeft dat derhalve impact, evenals dat dat organisatiekosten met zich meebrengt.

4.6 Impact financieel

4.6.1 Rijk

De Wdo heeft financiële consequenties en schetst de omgang daarmee (artikel 21):

- De kosten die het Rijk maakt, voor uitvoering van artikel 5 (digitale infrastructuur) en artikel 9 (toelaten van middelen) worden doorbelast aan bestuursorganen, aangewezen organisaties e.a.
- Bij ministeriële regeling volgen regels hierover (Regeling bekostiging), maar deze zijn nog niet gereed. Ook is bij BZK nog geen indicatie bekend van de omvang van de betreffende kosten.

Bestuursorganen

Bestuursorganen zullen zelf ook kosten maken vanwege de nieuwe wet- en regelgeving. Er is sprake van tijdelijke kosten en structurele kosten:

- Tijdelijke kosten maken organisaties om de wet- en regelgeving te implementeren. Het gaat dan zoal om kosten van implementatie van nieuwe verplichtingen (zoals de acceptatieplicht, het nemen van veiligheidsmaatregelen), aanpassing van ICT systemen (bijv. configuratie van HTTPS en HSTS), aansluiting en het wijzigen van bijbehorende werkprocessen.
- Structurele kosten hebben onder meer betrekking op de naleving van inhoudelijke verplichtingen (zoals borging van veiligheidsmaatregelen), uitvoering van het ICT beheer en logging en verplichtingen inzake informatieverstrekking/verantwoording.⁸

De hoogte van die kosten is op onderdelen afhankelijk van de mate waarin zij nu al voldoen aan de nieuwe verplichtingen. Dat verschilt tussen bestuursorganen. Sommige bestuursorganen hebben meer werk te doen dan andere bestuursorganen.

Bestuursorganen dragen bovengenoemde kosten die zij zelf maken in beginsel zelf, want zover bekend is hiervoor geen compensatie voorzien. Uitgangspunt is eveneens dat de publieke dienstverleners bij de verlening van hun diensten de kosten van identificatie en authenticatie dragen; het Rijk compenseert niet voor het feit dat zij als gevolg van dit wetsvoorstel hun digitale infrastructuur moeten aanpassen om de toegelaten en erkende identificatiemiddelen te kunnen accepteren (Memorie van Toelichting Wdo).

Met een aantal zaken wordt gewerkt aan het dempen van de meerkosten; met standaardisatie, de routeervoorziening en de cluster aansluiting. Hiermee tracht men de stijging van de kosten te beperken.

Naast kosten zullen dienstverleners ook baten genereren door het gebruik van een generieke, betrouwbare infrastructuur voor het digitaal inloggen, maar dat zijn niet baten met directe financiële consequenties.

Per saldo zal er sprake zijn van een kostenstijging voor bestuursorganen; het gaat om financiële kosten en administratieve lasten. Daarbij is de stijging van de financiële kosten relatief beperkt, omdat de wetgeving nu vooral een staande doch vrijblijvende praktijk (wettelijk) vastlegt. Er verandert daardoor niet zoveel qua kosten. Voor de administratieve lasten is dat een ander verhaal. De wet- en regelgeving brengt immers interbestuurlijk toezicht met zich mee en nieuwe verantwoordingsverplichtingen die er nu nog niet zijn (met uitzondering van DigiD). Dat leidt tot extra administratieve lasten.

⁸ Primair met betrekking tot interbestuurlijk toezicht. Er zijn geen nieuwe audit-verplichtingen te verwachten.

4.7 Tussenconclusies bestuur, organisatie en financieel

Bestuur. De impact van de Wdo op het bestuur is gering. De Wdo vereist een enkel besluit en het bestuur zal ruimte moeten creëren in de organisatie om aan de Wdo te kunnen voldoen. Daarbij helpt het als wettelijke verplichtingen op digitaal gebied duidelijk belegd zijn in de portefeuille van een bestuurder.

Organisatie. De impact van de Wdo op de organisatie is relatief beperkt. Het systeem en de bestaande verantwoordelijkheidsverdelingen in organisatie veranderen als zodanig niet. Wel komen er een aantal verplichtingen bij. Dat zal leiden tot een aantal initiële aansluittrajecten en in de beheersituatie tot een taakverzwaring voor het beheer en onderhoud van de verplichtingen die uit de Wdo voortvloeien.

Financieel. De Wdo zal zeker een financiële impact hebben en tot incidentele en structurele meerkosten leiden voor aansluitingen en voor het beheer en onderhoud. In generiek zin is het lastig om iets te zeggen over de omvang van deze kosten. Dat hangt voor een belangrijk gedeelte af van de uitgangspositie van het desbetreffende bestuursorgaan.

Interbestuurlijk toezicht. Het interbestuurlijk toezicht zoals dat nu voorligt in de Wdo is voor provincies niet uitvoerbaar. In de eerste plaats is nog veel niet voldoende gedefinieerd (zoals bijvoorbeeld de informatieverplichting). Maar bovenal roept het veel fundamentele vragen op over hoe de specifieke toezichtbepalingen zich verhouden tot het generieke toezicht van provincies. De Wdo reikt de provincies geen aanvullende instrumenten aan om naleving te bevorderen. En de vraag is of de bestaande generieke instrumenten voor de Wdo passend en toereikend zijn, in het dynamische werkveld van de digitale overheid. Dit introduceert een afbreukrisico voor gedeputeerde staten als toezichthouder op gemeenten en waterschappen. Ook vereist de Wdo capaciteit van specialisten op het gebied van informatiebeveiliging, privacy, dienstverlening en ICT. Deze kennis is in huis, maar is ingezet voor de eigen bedrijfsvoering.

BIJLAGE 1

Begeleidingsgroep en gesprekspartners

Begeleidingsgroep

- Paul Hogenhuis
- Jeroen Naterop
- Charlotte Dunnik
- Nicole de Keijzer

Begeleidingsgroep interbestuurlijk toezicht

- Ineke de Jonge, Provincie Groningen
- Roland Demmendaal, Provincie Noord-Holland,
- Marlies Houtman, Provincie Noord-Brabant,
- Dineke Meijering, Provincie Groningen,
- Peter Oosterhof, Provincie Overijssel
- Terri Quinn, Provincie Gelderland.

Gesprekspartners

- Sophia Büneman, BZK
- Robin Gelhard, Forum Standaardisatie
- Bart Knubben, Forum Standaardisatie
- Odette Bies, BZK
- Inge de Ruijter, BZK
- Lenne Huisman, Provincie Flevoland
- Andy Bramall, Provincie Flevoland
- Miriam van der Plas, Provincie Flevoland
- Hilko Batterink, Provincie Flevoland
- Stefanie Kelterman, Provincie Utrecht
- Casper Schutte, Provincie Utrecht
- Remco ter Heijne, Provincie Utrecht
- Rob de Lange, Rijnland
- Arjan Roorda, Noorder Zijlvest
- Ronald Holdijk, Rivierenland
- Roland Versluis, Waternet,
- Ada Karimlou, Brabantse Delta,
- Nalinie Omar, HHSK
- Albert van As, Rijnland



‘WIJ ZIJN BERENSCHOT, GRONDLEGGER VAN VOORUITGANG’

Wij zien een Nederland dat altijd in ontwikkeling is. Zowel sociaal als organisatorisch verandert er veel. Al meer dan 80 jaar volgen wij deze ontwikkelingen op de voet en werken we aan een vooruitstrevende samenleving. Daarbij staan we voor duurzaam advies en de implementatie hiervan. Altijd gericht op vooruitgang én echt iets kunnen betekenen voor mensen, organisaties en de maatschappij.

Alles wat we doen, is onderzocht, onderbouwd en vanuit meerdere invalshoeken bekeken. In ons advies zijn we hard op de inhoud, maar houden rekening met de menselijke maat. Onze adviseurs doen er alles aan om complexe vraagstukken om te zetten naar praktische oplossingen waar u iets mee kan. Wij geven advies en bieden digitale oplossingen waarbij we ons focussen op:

- Toekomst van werk en organisatie
- Energietransitie
- Transformatie van zorg
- Transformatie van openbaar bestuur

Berenschot Groep B.V.

Van Deventerlaan 31-51, 3528 AG Utrecht
Postbus 8039, 3503 RA Utrecht
030 2 916 916
www.berenschot.nl